INTELLIGENCE MEETS ENFORCEMENT: The Policy and Practice Benchmarks Arising from Inter-organisational Relationships Implemented to Address the “Wicked Issue” of Transnational Criminality in Denmark, Finland and New Zealand

Richard Stewart Shortt
Master of Public Management, Victoria University of Wellington, 2001
Diploma of New Zealand Policing, Royal New Zealand Police College, 1979

Doctor of Philosophy

Australian Graduate School of Policing and Security
Charles Sturt University

July 2015
STATEMENT OF AUTHORSHIP

This dissertation is submitted as fulfilment of the requirements for the degree of Doctor of Philosophy by research. I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the award of any other degree or diploma at Charles Sturt University or any other educational institution, except where due acknowledgment is made in the dissertation. Any contribution made to the research by colleagues with whom I have worked at Charles Sturt University or elsewhere during my candidature is fully acknowledged.

I agree that this dissertation be accessible for the purpose of study and research in accordance with the normal conditions established by the Executive Director, Library Services or nominee, for the care, loan and reproduction of theses.

............................................................

Richard Stewart Shortt
I wish to express my profound gratitude to the following people who assisted me in fulfilling my desire of undertaking the study presented herein.

Firstly, I wish to acknowledge Dr Henry (Hank) Prunckun, my supervisor. Hank guided me through the “scholarly labyrinth” which I, somewhat unwittingly, entered when the concept for this study formed following retirement from my career with New Zealand Police. Without Hank’s frank guidance, thoughtful advice, and willingness to share his accumulated experience I am confident I would not be where I find myself today.

Next, my gratitude is extended to the expert panel members who provided me with their time and thoughtful advice regarding the case studies on Denmark, Finland and New Zealand. They were: Ms Kira Rønn PhD, a strategic analyst at the National Center of Investigations within the Danish National Police, Mr Stefan Aniszewski, a former Finnish government employee and member of Finnish Customs, and Mr R Mark Evans OBE, Deputy Chief Executive, New Zealand Police. The involvement of those three individuals assisted in great measure to ensuring my descriptions of the environments within the three case study countries was as accurate as possible and absent of any bias that I may have brought to the process.

The next person I need to acknowledge is Dr Gareth Den Heyer. Gareth steered me towards Charles Sturt University and Henry Prunckun when he learnt of my desire to pursue a scholarly path. Gareth’s guidance proved to be correct.

Throughout the time it took me to complete this study, I was most fortunate to have the comradeship of the academics and staff working in the Canberra offices of the Australian Graduate School of Policing and Security, Charles Sturt University. Daily interaction with them turned an otherwise lonely journey into one that was enjoyable and collegial.

Finally, I acknowledge from the depths of my heart my best friend and partner: Leonie. Without her encouragement, support and love none of this would have been possible. It’s that simple really.
This study looks at how “wicked” security issues like transnational criminality (including both terrorism and transnational crime) were being responded to in three “intermediate capacity” countries. The study describes how governments, intelligence and law enforcement communities (or agencies) in Denmark, Finland and New Zealand structured and managed their inter-organisational relationships during the period 2007–2012.

The study’s literature review identified that six inter-organisational relationship types exist, and enabled the fundamental features of each to be identified so as to differentiate more clearly between each type. That knowledge was then used to assess the contents of publicly available secondary sources, gathered from official government websites or scholarly publications, detailing intelligence and law enforcement inter-organisational relationships in the three case study countries.

The case studies established that the inter-organisational relationships in the three countries involved a combination of cooperation, coordination and collaboration relationship types, using networked structures of multiple agencies to target specific “wicked” security issues such as terrorism, human trafficking or cyber attack/crime. Those results were then aggregated enabling a combined perspective of the findings. From that combined perspective a number of policy and practice benchmarks and implications were distilled.

The distillation revealed that four elements were either explicitly or implicitly evident across the countries studied, enabling the inter-organisational relationships observed to occur. The four elements were labelled: Permission, Leadership, Flexibility, and Adaptability. Government’s wishing to emulate the case study countries’ approach, need to begin by addressing the presence of those four elements in their own environments.
CONTENTS

STATEMENT OF AUTHORSHIP ................................................................. II
ACKNOWLEDGEMENTS ........................................................................ III
ABSTRACT ............................................................................................. IV
CONTENTS ............................................................................................ V
LIST OF FIGURES .................................................................................. VII
LIST OF TABLES ..................................................................................... IX
LIST OF ACRONYMS .............................................................................. X

CHAPTER 1 — INTRODUCTION ............................................................... 1
  BACKGROUND ...................................................................................... 1
  RATIONALE ......................................................................................... 2
  THEORETICAL BASE ........................................................................... 3
  RESEARCH QUESTION ......................................................................... 5
  APPROACH OF THE STUDY ............................................................... 5
  OUTLINE OF THE STUDY ................................................................. 6

CHAPTER 2 — LITERATURE REVIEW ....................................................... 8
  EMERGENCE OF THE TRANSNATIONAL CRIME THREAT .................. 8
  9/11 – A FOCUSING EVENT ............................................................ 10
  POLICY REVIEWS .............................................................................. 11
  NEW PARADIGMS, NEW RESPONSES ............................................. 13
  OPTIONS AND RESPONSES .......................................................... 14
  INTER-ORGANISATIONAL RELATIONSHIP TYPES ......................... 15
  RELATIONSHIP CONTINUUM ....................................................... 21

CHAPTER 3 — METHODOLOGY ............................................................... 27
  DATA GATHERING .............................................................................. 27
    Preparation for Case Study Selection ........................................... 27
    Case Study Data ............................................................................. 27
    Case Study Comparison ............................................................... 29
  DATA COLLATION AND ANALYSIS .................................................. 29
    Case Study Selection ................................................................. 29
    Case Studies General Overview ................................................. 32
    New Zealand Case Study ........................................................... 34
    Denmark Case Study ................................................................. 40
    Finland Case Study ................................................................. 47
    Case Study Comparison ........................................................... 55
  LIMITATIONS .................................................................................... 55
  ETHICAL ISSUES .............................................................................. 56

CHAPTER 4 — CASE STUDY RESULTS .................................................. 57
  OVERVIEW ......................................................................................... 57
  NEW ZEALAND .................................................................................. 57
    Government Relationship Expectations ..................................... 57
    Intelligence Community Relationships ..................................... 68
    Law Enforcement Community Relationships ........................... 74
    Limitations ..................................................................................... 78
  DENMARK .......................................................................................... 78
    Government Relationship Expectations ..................................... 78
LIST OF FIGURES

FIGURE 2.1. RELATIONSHIP CONTINUUM DIALS .................................................................................................... 26
FIGURE 4.1. NEW ZEALAND GOVERNMENT’S RELATIONSHIP EXPECTATIONS (N=99) ............................................. 58
FIGURE 4.2. NEW ZEALAND CENTRAL AGENCIES RELATIONSHIP EXPECTATIONS (N=86) ...................................... 59
FIGURE 4.3. NEW ZEALAND GOVERNMENT’S RELATIONSHIP STRUCTURE EXPECTATIONS (N=30) ......................... 59
FIGURE 4.4. NEW ZEALAND CENTRAL AGENCIES RELATIONSHIP STRUCTURE EXPECTATIONS (N=12) ............... 59
FIGURE 4.5. NEW ZEALAND GOVERNMENT’S EXTENT OF ENGAGEMENT EXPECTATIONS (N=34) .......................... 60
FIGURE 4.6. NEW ZEALAND CENTRAL AGENCIES EXTENT OF ENGAGEMENT EXPECTATIONS (N=18) ................. 60
FIGURE 4.7. NEW ZEALAND’S INTELLIGENCE COMMUNITY (IC) RELATIONSHIPS (N=228) .................................... 69
FIGURE 4.8. NEW ZEALAND’S IC RELATIONSHIP STRUCTURES (N=30) .................................................................. 70
FIGURE 4.9. NEW ZEALAND’S IC EXTENT OF ENGAGEMENT (N=42) ...................................................................... 70
FIGURE 4.10. NEW ZEALAND’S IC RELATIONSHIP MOTIVATIONS (N=37) ............................................................... 71
FIGURE 4.11. NEW ZEALAND’S LAW ENFORCEMENT COMMUNITY (LEC) RELATIONSHIPS .................................. 74
FIGURE 4.12. NEW ZEALAND’S LEC RELATIONSHIP STRUCTURES (N=21) .............................................................. 75
FIGURE 4.13. NEW ZEALAND’S LEC EXTENT OF ENGAGEMENT (N=31) ................................................................. 75
FIGURE 4.15. DANISH GOVERNMENT RELATIONSHIP EXPECTATIONS (N=76) ....................................................... 79
FIGURE 4.16. DANISH GOVERNMENT RELATIONSHIP STRUCTURE EXPECTATIONS (N=17) ..................................... 79
FIGURE 4.17. DANISH GOVERNMENT EXTENT OF ENGAGEMENT EXPECTATIONS (N=24) ....................................... 80
FIGURE 4.18. DANISH INTELLIGENCE COMMUNITY (IC) RELATIONSHIPS (N=54) .................................................. 84
FIGURE 4.19. DANISH IC RELATIONSHIP STRUCTURES (N=8) ............................................................................... 84
FIGURE 4.20. DANISH IC EXTENT OF ENGAGEMENT (N=6) .................................................................................... 85
FIGURE 4.22. DANISH LAW ENFORCEMENT COMMUNITY (LEC) RELATIONSHIPS (N=50) ..................................... 90
FIGURE 4.23. DANISH LEC RELATIONSHIP STRUCTURES (N=13) ......................................................................... 90
FIGURE 4.24. DANISH LEC EXTENT OF ENGAGEMENT (N=16) ............................................................................... 91
FIGURE 4.25. DANISH LEC RELATIONSHIP MOTIVATIONS (N=20) ................................................................. 91
FIGURE 4.26. FINNISH GOVERNMENT’S RELATIONSHIP EXPECTATIONS (N=106) ............................................... 94
FIGURE 4.27. FINNISH GOVERNMENT’S RELATIONSHIP STRUCTURE EXPECTATIONS (N=39) .............................. 94
FIGURE 4.28. FINNISH GOVERNMENT’S EXTENT OF ENGAGEMENT EXPECTATIONS (N=64) ................................. 95
FIGURE 4.29. FINNISH SECURITY SERVICE RELATIONSHIPS (N=5) .................................................................. 98
FIGURE 4.30. FINNISH SECURITY SERVICE RELATIONSHIP STRUCTURES (N=2) ................................................... 99
LIST OF TABLES

TABLE 2.1. SOURCES FOR INTER-ORGANISATIONAL RELATIONSHIP TYPE FEATURE DESCRIPTIONS ......................... 17
TABLE 2.2. “RESOURCE SHARING” MENTIONS AND COUNTER POINTS FOR EACH RELATIONSHIP TYPE .......... 18
TABLE 2.3. FEATURES OF RELEVANCE ACROSS ALL RELATIONSHIP TYPES .......................................................... 18
TABLE 2.4. FEATURES SHARED BY RELATIONSHIP TYPES ...................................................................................... 19
TABLE 2.5. FEATURES PRINCIPALLY ASSOCIATED WITH ONLY ONE RELATIONSHIP TYPE ................................. 19
TABLE 3.1. COUNTRY CAPACITY PARAMETERS AND DISTRIBUTION ........................................................................... 30
TABLE 3.2. COUNTRIES MEETING THE INTERMEDIATE PARAMETERS FOR ALL CRITERIA ........................................... 30
TABLE 3.3. COUNTRIES MEETING THE INTERMEDIATE PARAMETERS FOR THREE CRITERIA ........................................ 31
TABLE 3.4. CAPACITY DATA FOR COUNTRIES IN CASE STUDY SELECTION POOL .................................................... 31
TABLE 3.5. NEW ZEALAND CASE STUDY SOURCE DISTRIBUTION ........................................................................... 36
TABLE 3.6. NEW ZEALAND AGENCIES ................................................................................................................... 37
TABLE 3.7. NEW ZEALAND CASE STUDY DATA DISTRIBUTION ............................................................................... 39
TABLE 3.8. DENMARK CASE STUDY SOURCE DISTRIBUTION .................................................................................. 43
TABLE 3.9. DANISH AGENCIES ................................................................................................................................... 45
TABLE 3.10. DENMARK CASE STUDY DATA DISTRIBUTION .................................................................................... 46
TABLE 3.11. FINLAND CASE STUDY SOURCE DISTRIBUTION ................................................................................... 50
TABLE 3.12. FINNISH AGENCIES ............................................................................................................................ 53
TABLE 3.13. FINLAND CASE STUDY DATA DISTRIBUTION ...................................................................................... 54
TABLE 5.1. GOVERNMENT RELATIONSHIP EXPECTATIONS COMPARISON ............................................................. 107
TABLE 5.2. IC INTER-ORGANISATIONAL RELATIONSHIP COMPARISONS ............................................................... 111
TABLE 5.3. LEC INTER-ORGANISATIONAL RELATIONSHIP COMPARISONS ............................................................ 112
TABLE 5.4. GLOBAL PEACE INDEX RANKINGS FOR CASE STUDY COUNTRIES ....................................................... 114
TABLE 5.5. POSITIVE PEACE INDEX RANKINGS FOR CASE STUDY COUNTRIES ..................................................... 114
TABLE 5.6. CORRUPTION PERCEPTION INDEX RANKINGS FOR CASE STUDY COUNTRIES* .................................... 115
TABLE 5.7. GLOBAL TERRORISM INDEX RANKINGS FOR CASE STUDY COUNTRIES – 2012 ................................... 115
TABLE 5.1. INDICATIVE SUMMARY OF EXPERT PANEL MEMBERS’ RESPONSES ....................................................... 174
LIST OF ACRONYMS

GENERAL

7/7  7 July 2005, terrorist attacks on public transport in London, England
AFP  Australian Federal Police
AIC  Australian Intelligence Community
EU  European Union
FBI  Federal Bureau of Investigation, United States of America
GDP  Gross Domestic Product
G7  The Group of Seven – an informal bloc of industrialised democracies comprising: the United States of America, Canada, France, Germany, Italy, Japan, and the United Kingdom
G20  Group of the 20 largest economies in the world
HREC  Human Research Ethics Committee, Charles Sturt University
IEP  Institute for Economics and Peace
IC  Intelligence Community
LEC  Law Enforcement Community
NC3  Networking, Cooperation, Coordination, and Collaboration
NPM  New Public Management
NZ  New Zealand
OECD  Organization for Economic Cooperation and Development
RC  Relationship Continuum
UK  United Kingdom
USA  United States of America
USD  United States Dollar

DENMARK

CFCS  Center for Cyber Security (Danish acronym)
CTA  Center for Terror Analysis
DEMA  Danish Emergency Management Agency
DK1  Denmark Case Study Data Set 1
DK2  Denmark Case Study Data Set 2 (a subset of DK1)
Europol  European Police Office
FE  Forsvarets Efterretningstjeneste (Danish Defence Intelligence Service)
MLS  Money Laundering Secretariat
NATO  North Atlantic Treaty Organization
NEC  National Centre of Investigations (Danish acronym)
NOS  National Operative Staff
PET  Politiets Efterretningstjeneste (Danish Security and Intelligence Service)

FINLAND
FD1  Finland Case Study Data Set 1
FD2  Finland Case Study Data Set 2 (a subset of FD1)
FIRE  Finnish Intelligence Research Establishment
FIS  Finnish Immigration Service
ILO  Immigration Liaison Officer
ISP  Internal Security Programme
NBI  National Bureau of Investigation
NGO  Non-Governmental Organisation
OSCE  Organisation for Security and Co-operation in Europe
PCB  Police, Customs and Border Guard (acronym for ‘PTR’ used in Finnish documents translated into English)
PTR  Poliisi, Tulli and Rajavartiolaitos (Police, Customs and Border Guard)
Supo  Suojelupoliisi (Finnish Security Intelligence Service)

NEW ZEALAND
CPJS  Counter Proliferation Joint Section
CTAG  Combined Threat Assessment Group
DES Committee  Domestic and External Security Committee of Cabinet
DESC  Domestic and External Security Coordination
DESG  Domestic and External Security Group
DOL  Department of Labour
DPMC  Department of the Prime Minister and Cabinet
GCSB  Government Communications Security Bureau
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICG</td>
<td>Intelligence Coordination Group</td>
</tr>
<tr>
<td>ITOC</td>
<td>Integrated Targeting and Operations Centre</td>
</tr>
<tr>
<td>MED</td>
<td>Ministry of Economic Development</td>
</tr>
<tr>
<td>MFAT</td>
<td>Ministry of Foreign Affairs and Trade</td>
</tr>
<tr>
<td>NAB</td>
<td>National Assessments Bureau</td>
</tr>
<tr>
<td>NAC</td>
<td>National Assessments Committee</td>
</tr>
<tr>
<td>NZ1</td>
<td>New Zealand Case Study Data Set 1</td>
</tr>
<tr>
<td>NZ2</td>
<td>New Zealand Case Study Data Set 2 (a subset of NZ1)</td>
</tr>
<tr>
<td>NZ3</td>
<td>New Zealand Case Study Data Set 3 (a subset of NZ2)</td>
</tr>
<tr>
<td>NZDF</td>
<td>New Zealand Defence Force</td>
</tr>
<tr>
<td>NZIC</td>
<td>New Zealand Intelligence Community</td>
</tr>
<tr>
<td>NZSIS</td>
<td>New Zealand Security Intelligence Service</td>
</tr>
<tr>
<td>ODESC</td>
<td>Officials Committee for Domestic and External Security Coordination</td>
</tr>
<tr>
<td>OFCANZ</td>
<td>Organised and Financial Crime Agency New Zealand</td>
</tr>
<tr>
<td>SoI</td>
<td>Statement of Intent</td>
</tr>
<tr>
<td>SRG</td>
<td>Security Risk Group</td>
</tr>
<tr>
<td>SSC</td>
<td>State Services Commission</td>
</tr>
</tbody>
</table>
BACKGROUND

Scholars concur that transnational crimes—crimes spanning borders, exploiting gaps between national jurisdictions and impacting multiple states—are not a new phenomenon (Albanese, 2012, p. 3; Naim, 2006, pp. 3–8; Picarelli, 2012, p. 192 citing Andreas, 2004; Roth, 2014, p. 7). However, the international terrorist attacks on 11 September 2001 (9/11) in the United States had “spectacular symbolic” and “physical power” impacts (Hogg, 2007, p. 93). Those impacts resulted in western nations becoming even more focused on transnational criminal issues as they entered the twenty-first century (Aldrich, 2011, pp. 19–20).

The 9/11 attacks, and the resulting decade-long concentration by policymakers and scholars on international terrorism and its ally transnational crime (Archer, 2005, p. 398; Pickering, McCulloch, & Wright-Neville, 2008, p. 1) consolidated the already identified linkages between the two (Brodeur, 2005, p. 805; Greener-Barcham, 2002, p. 511; Naim, 2006, p. 7). Makarenko (2004, p. 130) used “converge[nce]” to describe the linkages between the phenomena of transnational crime and terrorism, a view supported by other scholars (for example, see Goldsmith, 2012, p. 278; Hoffman, 2010, p. 41; Martin, 2014, p. 245; West, 2013, pp. 115–116). To put convergence into context, Makarenko (2004, p. 130) argued both phenomena shared similar “operational and organisation” traits (a view supported by Hoffman, 2010, p. 40), while West (2013, p. 116) posited that there was now a “fusion” between “transnational organised crime groups” and “terrorist organisations.”

Transnational crime and international terrorism shared another common trait: they were both akin to the “wicked” problems described by Rittel and Webber (1973, pp. 160–167). In that work Rittel and Webber (1973, p. 160) described “wicked” problems as:

… “wicked” not because these properties are themselves ethically deplorable. We use the term “‘wicked’” in a meaning akin to that of “malignant” (in contrast to “benign”) or “vicious” (like a circle) or “tricky” (like a leprechaun) or “aggressive” (like a lion, in contrast to the docility of a lamb).

They were, therefore, difficult for policymakers and those charged with implementing policy to grapple with (Picarelli, 2012, p. 181; Walsh, 2011, p. 250; Whelan, 2012, p. 54; Wood, 2006, p. 249). Their “wickedness” stemmed from them being both cross-border in nature and activities that impacted multiple government agency mandates (Goldsmith, 2012, pp. 275–276). The “wickedness” was exacerbated by having often hard to define (or unpalatable) solutions, which in turn can give rise to unexpected and undesired consequences (Fleming & Wood, 2006, p. 2; Roth, 2014, p. 17). As a result of those challenges, governments began including both transnational crime and terrorism in their lists of national security issues (de Spiegeleire, 2013; Goldsmith, 2012, p. 295; Leigh, 2011, pp. 3–4; Makarenko, 2004, p. 130; Picarelli, 2012, p. 184; Sheptycki, 2009, p. 372; Whibley, 2013, p. 3).

Building on the views above, and the fact that terrorism had long been classified as a criminal act (Brodeur, 2005, p. 805; Foley, 2009, p. 441), this study adopted the term transnational criminality to encompass all criminal acts that crossed borders, exploited jurisdictions, and impacted multiple state agencies. In essence the term picked up Picarelli’s...
commentary of criminality being “ubiquitous within the crime-terror overlap” (2012, p. 194) and was very similar to the definition used by Harfield (2008, p. 485) in his article on organising organised crime policing. Other transnational crimes that fell within the term’s definition included: arms and people trafficking, piracy, narcotics smuggling, money laundering, illegal cyber activity, child sex tourism and corruption (Ash, 2013, p. 2; Harfield, 2008, p. 485; Roth, 2014, p. 18).

Arguably, the 9/11 and post-9/11 terrorist attacks that occurred during the first decade of the new millennium—very stark acts of transnational criminality—provided highly visible “focusing events” (Birkland, 2004, p. 181) in the national security policy environment. Those events “opened the policy window” (Birkland, 2004, p. 181; Zegart, 2007, p. 169), allowing governments to reassess their preparations and responses to not just terrorism, as a specific crime type, but also to the broader issue of transnational criminality. In several of the countries directly affected by terrorism, the opened policy window resulted in reviews to identify how state agencies should work and be configured in order to address the new national security agenda (for example, see Archambault, 2010, pp. 89–90), to the detriment of focus on more traditional forms of criminality some believe (Harfield, 2008, pp. 499–500; Moor, 2015).

The most wide-ranging and detailed review undertaken was in the United States of America (USA) by a congressional commission. The commission’s recommendations, reported back in 2004 (Kean et al., 2004), had at their heart the concept of unity of effort between all elements of government responsible for protecting the nation. Unity of effort called for, among other things, intelligence and law enforcement agencies to work more closely together. The recommendations suggested greater sharing of information and provision of a united front against terrorists (Kean et al., 2004, pp. 418 & 425–427).

Other review processes elsewhere in the world presented their governments with similar concepts, in particular, in Australia (Flood, 2004) and the United Kingdom (UK) (Intelligence & Security Committee, 2006). However, while identifying the need for intelligence and law enforcement communities to work more effectively together, no guiding outlines or benchmarks on how to do that emerged.

RATIONALE

More than a decade has passed since the dramatic series of events at the beginning of the twenty-first century. Reviews into 9/11 and other terrorist attacks have been completed and recommendations presented. As mentioned, a recurrent theme emerged from the reviews concerning the need for effective inter-organisational relationships. That was particularly so between intelligence and law enforcement agencies if they were to effectively prevent and respond to “wicked” security issues (Fleming & Wood, 2006, pp. 1–2; Hoffman, 2010, p. 41; Kearns et al., 2004, pp. 417–473; Whelan, 2012, p. 54). Governments—those initiating the reviews and those observing in order to learn from the experiences of others—have had ample opportunity to assess the reviewers’ findings, make decisions about those findings, and implement changes if needed.

It was, therefore, considered timely to study inter-organisational relationships between intelligence and law enforcement agencies to determine how they were being conducted. Furthermore, following a thought provoking presentation by Stephan de Spiegeleire
from The Hague Centre for Strategic Studies (de Spiegeleire, 2013) on national security risk management, in which he held that:

[the age of a ‘lines’ dominated world (i.e. borders and organisational boundaries) was shifting to one dominated by ‘flows’ and networks’] will also require a fundamental change in the way that our governments structure themselves, in the way they do strategic planning and in the way that they think about national security … breaking through stovepipes … I personally think that small countries should have a comparative advantage at this kind of stuff if you talk about the inter-agency piece, most of our small countries try to behave like big countries, the stovepipes are almost as big, as powerful, as secluded as silos … as they are in big countries. … small entities, whether they are economic or political, should have much more sensitivity for their environment, should have more agility in being able to turn things around … My suggestion is that … governments restructure themselves in new ways to deal with the complexities that are out there, that our thinking also changes to thinking much more in terms of ecosystems and in terms of outside in, rather than rigid stovepipes and inside out.

Interest was aroused regarding focusing the study on inter-organisational relationships occurring in what might be considered “small countries.” Those countries may, through de Spiegeleire’s perceived “sensitivity” and “agility”, it was posited, approach responding to “wicked” security issues in ways that were different to countries such as the USA, UK, and Australia.

As a consequence, this study, through exploration of intelligence and law enforcement relationships in “small countries,” and description of the inter-organisational relationships observed, aimed to identify and articulate policy and practice benchmarks that similarly positioned countries could apply. The benchmarks and any associated implications could assist if a government wished to critique its inter-organisational arrangements concerning transnational criminality. Alternatively, they could be used to help formulate policy for the development of new inter-organisational arrangements where a need for change was already identified.

THEORETICAL BASE

An outcome of the acknowledgement of “wicked” issues existing in the national security arena was the realisation that such problems could not be solved by one agency alone (Andrews & Entwistle, 2010, p. 681; Fleming & Wood, 2006, p. 2; Whelan, 2012, p. 15). As described by Rittel and Webber (1973) “wicked” issues needed to be examined from many perspectives before attempting to solve them, while accepting that ultimately there was no one right solution. At the same time one needed to be conscious that the solutions, when implemented, “will generate waves of repercussions” which in turn will need to be examined and responded to (Rittel & Webber, 1973, pp. 160–164). Since “wicked” issues do not fit neatly into one agency’s mandate (Agranoff & McGuire, 2001, p. 319), they do not, therefore, fit well with the traditional model of government bureaucracy. That model consisted of building functional-focused, siloed agencies, with specific mandates, specialised expertise, and limited overlap with other government entities (Christensen & Lægreid, 2007, p. 1060; Ryan & Walsh, 2004, p. 621).

In some countries, particularly Anglo-Saxon ones, that traditional bureaucratic model was adjusted during the 1980s and 1990s through implementation of New Public Management
(NPM) theory (Christensen & Lægreid, 2007, p. 1059). NPM theory further embedded the separation of agency mandates, introduced performance management concepts—including performance measures—to the public sector, and “ignored the problems of horizontal coordination” (Fimreite & Lægreid, 2005 as cited in Christensen & Lægreid, 2007, p. 1060; Harfield, 2008, p. 494). The unexpected and undesired consequences of NPM, when coupled with traditional bureaucratic models, were the fragmentation and siloed vertical structures found within public sectors and competition between what were perceived to be competing agencies (Harfield, 2008, p. 494). Those consequences increased the challenge of responding to “wicked” issues that required horizontal responses (Boston & Eichbaum, 2005 as cited in Christensen & Lægreid, 2007, p. 1060; Ryan & Walsh, 2004, p. 623).

In the mid-to-late 1990s, in response to fragmented public sectors and “wicked” policy issues, governments resorted to encouraging agencies to form networks and to work together using various inter-organisational arrangements (Christensen & Lægreid, 2007, p. 1061; McGuire, 2006, p. 33; Turrini, Cristofoli, Fro, & Nasi, 2010, p. 528). New terms to describe those adjusted working arrangements, such as whole-of-government and joined-up government, were coined and added to the lexicon of public servants and their political leaders (Christensen & Lægreid, 2007, pp. 1059–1060). The relationship arrangements that resulted from those new ways of working were often voluntary (but encouraged) in nature, while some were imposed by legislation (Doig, 2005, pp. 426–427; Muijs, West, & Ainscow, 2010, p. 16; Wood, 2006, p. 249). Some agencies, however, for a variety of reasons, including tradition and turf protection, failed to adapt to the new working arrangements (Brodeur, 2010, p. 214; Davies, 2004, p. 517; Doig, 2005, p. 426; McGuire & Agranoff, 2011, p. 268; Plamping, Gordon, & Pratt, 2000, para. 2; Zegart, 2007, p. 79).

Organisational fragmentation between government agencies with responsibility for national security, particularly intelligence and law enforcement agencies, was, for example, further aggravated by long-standing operational practices. Those practices included the “need to know” principle that restricted flows of information, compartmentalisation of activities that allowed for duplication of effort (or none at all when one agency thought another was responsible), and demarcation between domestic and foreign responsibilities which created exploitable gaps (Aldrich, 2011, pp. 26 & 32; Bamford, 2004, pp. 750–751; Hoffman, 2010, p. 46; Lowenthal, 2012, p. 49; Persson, 2013, pp. 16–17; Svendsen, 2008, pp. 663–664; Zegart, 2007, pp. 68 & 112–113).

In the national security realm, it took the crises of 9/11 and the subsequent terrorist attacks of the early 2000s to highlight the need for intelligence and law enforcement agencies to work more closely together—including those that were already doing so (Archambault, 2010, pp. 89–90; Bamford, 2004, p. 745; Lowenthal, 2012, p. 26; Manningham-Buller, 2007, pp. 44–45; Roach, 2010, p. 49). Spurred on by the findings of various reviews, and acknowledgement of the changed security environment, intelligence and law enforcement agencies were set the challenge of creating new or improved inter-organisational relationships and supporting arrangements (Clarke, 2007, paras. 17–19; Northcott, 2007, pp. 472–473; Omand, 2009, p. 396; Treverton, Wollman, & Wilke, 2011, p. 120). Put another way, horizontal coordination was firmly back on the agenda.

Inter-organisational relationships—in the public and private sectors—have been the subject of scholarly study for many years (Arnstein, 1969; Axelrod, 1984). As knowledge about
inter-organisational relationships developed it became clear there were a finite set of relationship types from which organisations could chose (Cigler, 2001, pp. 74–76; Eppel et al., 2008; Himmelman, 2002, pp. 2–4; Mattessich & Monsey, 1992, p. 42). As well as identifying specific relationship types, scholarly study identified the structures within which the relationships operated (i.e. dyadic or networked) (McGuire & Agranoff, 2011, p. 280; Fleming & Wood, 2006, p. 3), and the extent (or depth) to which various relationship types could be taken (Smith & Wohlstetter, 2006, p. 254; Thomson & Perry, 2006, p. 23).

RESEARCH QUESTION

Many countries now faced the challenge of managing “wicked” security issues that impacted upon their policy environments. Not the least challenging of those was the growth of transnational criminality attributed by some to increased globalisation and expanding use of technology. Given that challenge, the question that presented itself was: What types of inter-organisational relationships have developed between intelligence and law enforcement communities in intermediate capacity countries in an effort to address the “wicked” issue of transnational criminality, and can the study of those relationships lead to policy and practice benchmarks for other similarly situated countries to consider?

APPROACH OF THE STUDY

This study used a qualitative research methodology that was supported by quantitative analysis. The initial focus of the work was confirmation of what inter-organisational relationship types existed from study of the scholarly literature. Through reviewing the literature it was possible to construct a set of mind maps, one for each of the common relationship types identified. Those relationship types were then situated on a relationship continuum (RC) to determine how they related to one another and to other elements of inter-organisational relationships, such as the structures supporting the relationships, and the extent (or depth) of engagement occurring in each relationship.

With the mind maps and RC as reference points, three case studies of intermediate capacity countries—following the approach to such research described by Yin (2009)—were embarked upon. To select the case study subjects, data sets were gathered to help stratify the world’s 193 countries into large, intermediate and small capacity groupings. The intermediate grouping was then assessed against a set of criteria to choose three countries that were suitably similar, but geographically dispersed, to be the subjects for the case studies.

Sources for the case studies were gathered for the time period 1 January 2007 to 31 December 2012. The rationale for selecting that period was three-fold: (1) it avoided the period of ‘settling down’ following the 9/11 and subsequent terrorist attacks during which a number of reviews were undertaken exploring the nature and effectiveness of intelligence and law enforcement relationships; (2) it allowed time for the reviews’ findings, reported back over the period 2004–2007 (for example, see Kean et al., 2004; Flood, 2004; Street, Brady, & Moroney, 2006, p. 27)
to be operationalised and reflected in national security arrangements by the governments involved, or by observer countries (for example, the intermediate capacity subjects of this study); and finally, (3) it provided a time period containing a manageable volume of secondary data to support the research (Silverman, 2010, p. 55).

The case studies relied on secondary data in the form of text–based documents. The documents were sourced from publicly accessible official websites maintained by the case study countries’ governments and official agencies. The source documents were subjected to a multiple reading process. The process located text referring to inter-organisational relationships between intelligence and law enforcement agencies relating to the issue of transnational criminality. Review of the located text then enabled the identification of the relationship types involved and referred to earlier. The data discovered from the readings was then coded, extracted and placed in a spreadsheet for analysis.

Analysis of the data included both quantitative and qualitative assessment approaches. The quantitative analysis used the number of identifications of each relationship type (and structures and extent of engagement) to inform findings on how each country arranged their relationships. The qualitative analysis then focused on describing the context around the identified relationships to support (or challenge) the quantitative findings and to expand upon them.

The methodology and sources of data were chosen for three reasons. Firstly, they were appropriate to the research question. Secondly, they were manageable by the researcher. Finally, the data sources overcame two limitations presented by the research question, namely the issue of secrecy surrounding the workings of intelligence communities (Brodeur, 2010, p. 185), and exploration of a timeframe that included a historical as well as more contemporary context (May, 2001, p. 176; O’Leary, 2010, p. 128; Silverman, 2010, pp. 9–10).

OUTLINE OF THE STUDY

Chapter 2 presents the literature review covering the emergence of transnational crime as a security threat and the impacts of 9/11 and subsequent terrorist attacks. It discusses the general changes those two phenomena initiated in the realm of national security inter-organisational arrangements. The chapter examines how the threat posed by transnational crime emerged in the late 1990s following the demise of the former Soviet Union. It also describes how the terrorist attacks of the early 2000s provided a “focusing event” that allowed policymakers to re-consider how intelligence and law enforcement agencies should interact given the changes in the threat environment. The chapter goes on to identify and describe the various inter-organisational relationship types revealed during the study of scholarly works. It confirms that six different relationship types exist and provides detail on the features of each type. It reveals that some features are shared between relationship types, while others are principally associated with only one relationship type. The chapter also presents a diagram (Figure 2.1) that shows how the types relate to each other, the structures underpinning inter-organisational relationships, and the extent to which inter-organisational engagement can be taken for each relationship type.
Chapter 3 describes the methodology used for this study. The chapter details how the three countries for the case studies were selected, including a description of the data sets used to stratify the 193 countries of the world into three broad groupings: large, intermediate, and small capacity. It also outlines the criteria used to make the final selection of case study countries from the pool of potential subjects. The chapter then describes the general methodology applied to the case studies, including the use of a panel of experts to critique the case study descriptions. It then provides detail about the specific methodology concerning each of the individual cases given they involved countries using three different languages and differing bureaucratic structures. The chapter concludes by describing the limitations applicable to the studies and the ethical issues faced.

Chapter 4 presents the three case studies. The first study is on New Zealand, which was used as the pilot study. The analysis results are presented as a series of charts, accompanied by discussion of the context surrounding the data and of particularly enlightening sources. The case study concludes with discussion of the results and the findings arising from them. The same format is then repeated for the case studies regarding Denmark and Finland.

Chapter 5 contains a comparison and discussion of the three case studies’ results. It describes the similarities and differences discovered between the three. The chapter concludes with a presentation of policy and practice benchmarks and considerations identified through the discussion.

Chapter 6 presents the conclusions reached from this research. The conclusions cover the comparative findings from the case studies and the elements identified as present in the three case study countries that allowed the observed inter-organisational relationships to occur. The chapter sets out views on additional research that could follow on from this study, and reiterates the limitations that should be borne in mind concerning the study and its findings.
CHAPTER 2 — LITERATURE REVIEW

EMERGENCE OF THE TRANSNATIONAL CRIME THREAT

Transnational crime is not new (Albanese, 2012, p. 4; Naim, 2003, p. 29; Roth, 2014, p. 7; West, 2013, p. 116). What was considered recent however, and principally a feature of the past two decades (Albanese, 2012, p. 4), was the “scale, ability, and ease with which new, often networked and flexible organisations” (West, 2013, p. 116) were able to engage in transnational crime. Globalisation, with its increase in trade, improved communication systems, expansion of travel opportunities and the subsequent mass movement of people, has been cited as contributing to the evolution and emergence of transnational crime as a modern day threat (Albanese, 2012, p. 3; Leigh, 2011, p. 3; Naim, 2003, pp. 29–30; Roth, 2014, p. 7; West, 2013, p. 114 citing Gillman et al.). Scholars have also identified the demise of the former Soviet Union and the weaknesses in new democracies as additional contributing factors to the movement of organised crime from simpler, localised forms to a more complex transnational manifestation (Albanese, 2012, p. 4; Leigh, 2011, p. 3; Makarenko, 2004, pp. 140–141).

Albanese (2012, p. 3) succinctly defined organised crime, drawing on the “common elements of multiple scholars” as:

A continuing criminal enterprise that rationally works to profit from illicit activities that are often in great public demand. Its continuing existence is maintained through the use of force, threats, monopoly control, and/or corruption of public officials.

He went on to expand on that definition to describe transnational crime as:

A form of organized crime given its multi-national aims and the extent of organization required for success. Transnational organized crime can be considered the modern extension of organized crime in the globalized era. (2012, p. 3)

Albanese’s definition is similar to one presented earlier by Shelley (Goldsmith, 2012, p. 277, citing Shelley, 1999, p. 26).

The extent to which organised crime, and its modern variant transnational crime, were of growing international concern was evident when, in 1994, the Group of Seven (G7) heads of state and the European Union’s president “expressed ‘alarm about the growth of organised transnational crime …’” (Mitsilegas, 2003, pp. 75–76). A relatively short time later (in political terms), the United Nations drafted the Convention Against Transnational Organized Crime in December 2000 (Albanese, 2012, p. 11). Following drafting, the convention was ratified in 2003 and subsequently, Albanese reported, 171 of the United Nations 193 member countries had signed up to the convention (2012, p. 11).

Beyond the concerns of the G7 and the United Nations, the threat perceived regarding organised crime and transnational crime was being reflected regionally in various ways. For example, in Europe, the European Police Office (Europol) was created in 1995 as a direct counter to organised crime within the expanding European Union (Brady, 2007, p. 4; Godson & Williams, 1998, p. 72), while in the Nordic states (Denmark, Finland, Norway, and Sweden) various agreements and operational mechanisms had been developed to counter cross-border crime (Myrdal, 2005, pp. 96–97).
The rise in concern regarding transnational crime (as well as international terrorism) was also giving rise to new ways of working for intelligence and law enforcement agencies. Intelligence agencies were described as moving from “finding” (information) to more of a “fixing” and ‘enforcing’ mandate (Aldrich, 2011, p. 20), while law enforcement was being required to adopt a greater intelligence-led focus (2011, p. 20). Furthermore, security intelligence agencies—traditionally focused on internal/domestic issues—were now becoming more involved in establishing links with a wider range of international counterparts given that threats to a country could emanate from even the “smallest states” (Aldrich, 2011, p. 32). For example, in the United Kingdom (UK), in 1994, the Intelligence Services Act was enacted to empower the British Secret Intelligence Service (also known as MI6) and the Government Communications Headquarters (GCHQ) to exercise their powers, amongst other things, “in support of the prevention or detection of serious crime” (Omand, 2011, pp. 399–400).

While MI6’s sibling agency, the domestically focused British Security Service (also known as MI5) became directly involved with supporting law enforcement in the “detection and prevention of serious crime” in 1996 (Northcott, 2007, p. 459). Some, like O’Reilly and Ellison (2006, p. 646) argued that the shift of intelligence agencies focus from “high policing” to “criminal activities traditionally associated with low policing” (Brodeur, 2007, p. 27) was simply a means by which intelligence services could “locate new legitimising security threats (e.g. organised crime, right wing extremism).” Others, however, saw the shift as a necessary move to confront a growing and concerning threat (Aldrich, 2011, p. 19; Godson & Williams, 1998, pp. 66–67; Leigh, 2011, p. 3). Linked to that new and concerning threat was the concept of “convergence” as described by Bigo (2000, pp. 171–172). Convergence was “external security agencies … looking inside the borders in search of an enemy from outside… [and] … internal security agencies … looking to find their internal enemies beyond the borders.”

On the law enforcement side of the issue, the establishment of the International Criminal Police Organization (Interpol)—both an “international security network” and an “informational or virtual security network” (Dupont, 2007, pp. 80–82)—in 1923 showed that cooperation against organised transnational crime was not a new phenomenon (Godson & Williams, 1998, p. 71). However, with the increase in scale and scope of transnational crime additional law enforcement resources and arrangements were considered necessary. Europol—mentioned earlier—was one such initiative, as was the 1995 move by the G7 heads of state to initiate the “Senior Experts Group on Transnational Crime” (1998, p. 73) to provide recommendations on how to tackle the threat to their yearly meetings. At about the same time, in 1996, the Council of Baltic Sea States (Denmark, Finland, Germany, Sweden, Estonia, Latvia, Lithuania, Poland, Russia, Norway, and Iceland) determined that action was needed in regards to organised and transnational crime. They, in concert with the presidents of the EU commission and European Council established the “Task-Force on Organized Crime in the Baltic Sea Region” (Ulrich & Kivimaki, 2002, pp. 10–11). The task force was to “assess the threat of organised and transnational crime in the region and … formulate proposals for combating crime on the operational level” (2002, pp. 10–11, 21).

While transnational crime had been identified as a key threat, and had been elevated in status to a national security issue by some (Brady, 2007, p. 4; Godson & Williams, 1998, p. 67; Goldsmith, 2012, p. 295; Sheptycki, 2009, p. 372), it had only resulted in what were arguably “lite,” or perhaps even tentative, relationships between intelligence and law
enforcement agencies. Despite transnational criminals (and terrorists) resorting to modern techniques of communication and covert financing, which intelligence agencies special skill sets may be well suited to attacking (Omand, 2009, p. 396), transnational crime had not, it is posited, engendered a deeper strategic rethink of the relationships between what have been traditionally separate—but symbiotic—communities (West, 2013, p. 115; Wark, 2010, p. 168. That situation changed in September 2001.

9/11 – A FOCUSING EVENT

The events of 11 September 2001 (9/11) in the USA were a shock to people around the world, not least to citizens of countries a world away from what took place (Clark, H., 2002a; Goff, 2001). For example, the then New Zealand Prime Minister spoke of the events as being of momentous importance, involving the world’s superpower being attacked, not by another nation, but by a “multinational network” (Clark, H., 2001, n.p.).

Clearly, the international security environment had been irrevocably changed by such events. International (transnational) terrorism became a high priority for nations (Clark, H., 2002b; Goff, 2001; Karlsson, 2012, p. 38; Teirilä, 2015, p. 220; Wark, 2010, p. 174). Birkland’s definition of a “focusing event” (1997, p. 22) ably fits the circumstances presented by 9/11. The attacks presented an opportunity for change to policymakers through “opening of the policy window” (Birkland, 2004, p. 181; Zegart, 2007, p. 169) on national security arrangements. By opening that window, not only could international terrorism be reviewed, but also the convergent allied issue of transnational criminality (Makarenko, 2004, p. 130; Picarelli, 2012, p. 181), to which terrorism was being increasingly linked (Martin, 2014, p. 243). The overall effect was to allow inter-organisational relationship arrangements to be reassessed and if necessary adjusted.

Of specific relevance to this study was the assessment and adjustment, if necessary, of inter-organisational relationships between intelligence and law enforcement agencies. 9/11 and the terrorist events preceding it—such as the bombing of Air India flight 182, and the expansion in scale of transnational criminal activity (Roth, 2014, p. 7), had brought into focus the “blurring” of what has been described as the “traditional” foreign-domestic divide between what intelligence agencies (foreign, signals, and security) and law enforcement agencies dealt with (Brodeur, 2005, p. 805; Lowenthal, 2012, p. 49; Roach, 2010, p. 59; Omand, 2009, p. 396). Another outcome from terrorist activity for law enforcement—especially the emergence of complex mass-casualty attacks—was an increased focus on prevention as opposed to the traditional role of response (for example, see Husabø, 2013, pp 3–4). While community policing initiatives in the 1980s and 1990s had moved law enforcement in several western countries towards a more solutions-based crime prevention approach (Holmberg, 2013, p. 3; O’Connor, 2006b, pp. 42–43; McGarrell, Freilich, & Chermak, 2007, pp. 143–144); the threat of deadly acts by extremists ratcheted up the pressure to be intelligence-led and to get ahead of any future attacks (Murdoch, 2009, pp. 5–6; Street et al., 2008, p. iv; Taylor & Russell, 2012, pp. 184–185; Theoharis, 2007, p. 3). The need for intelligence to inform the prevention approach contributed, it is posited, to bringing relationships between intelligence agencies (high policing) and law enforcement (low policing) to the forefront of the debate on how to effectively structure national security arrangements, or the “new securitization” as Bigo (2000, pp. 171–172) termed it.
Countries, particularly those directly impacted, took the opportunity presented by terrorist attacks to review and adjust their national security arrangements. They included, for example, the USA, the UK, Australia, and Canada.

In the USA the response to 9/11 included establishment of a bi-partisan commission (the National Commission on Terrorist Attacks Upon the United States) to enquire into the events and to report on how they happened. The commission also sought to prevent any repeats (Kean et al., 2004, p. xv). Amongst the resulting inter-organisational relationship recommendations were four that aimed to underpin what the commissioners considered was the need for a “different way of organising the Government” (Kean et al., 2004, pp. 399–400). At the heart of those particular recommendations was the concept of unity of effort. In using that term the commissioners’ sought to convey the style of performance they desired from operational agencies and the government as a whole (Kean & Hamilton, 2006, p. 288), given the commission’s view that the current arrangements were based on historical threats and had failed to meet modern needs (Kean et al., 2004, p. 399). The four recommendations underpinning unity of effort involved:

- unifying strategic intelligence and operational planning … across the foreign-domestic divide with a National Counterterrorism Centre; unifying the intelligence community with a new National Intelligence Director; unifying the many participants in the counterterrorism effort and their knowledge in a network-based information-sharing system that transcends traditional government boundaries; … strengthening the FBI and homeland defenders. (Kean et al., 2004, pp. 399–400)

Across the Atlantic in the UK, despite its history of tackling Irish terrorism, there was not an initial awareness of the scope and nature of the new threat from Islamic extremists (Andrew, 2009, p. 814). Nor was there immediate appreciation that it would drive the need for a different way of doing business by the intelligence and law enforcement communities (Clarke, P., 2007, para. 9–10). However, in 2003, Operation CREVICE—the thwarting of an Islamic extremist bombing campaign against nightclubs, pubs and shopping centres (Andrew, 2009, p. 846)—changed that thinking. An appreciation dawned that attacks by Islamic extremists against the UK were possible. Furthermore, it had become apparent that “home-grown” extremists existed in the country—notwithstanding earlier revelations of Islamic extremist capabilities from what was known as “the Ricin Plot” (O’Neill & McGrory, 2006, p. 238).

Realisation of the UK’s fear came on 7 July 2005. Four “home-grown” Islamic extremist suicide bombers exploded improvised devices on three underground trains and a bus in central London (Andrew, 2009, p. 821; Pickering et al., 2008, p. 38). Those attacks were followed 14 days later by a failed set of similar attacks by a separate group of “home-grown” Islamic extremists. Subsequently, a parliamentary committee was tasked with enquiring into the events of July 2005 and it reported back in May 2006 (Murphy et al., 2006).

On the issue of intelligence and law enforcement engagement, the committee found the intelligence community—with particular the British Security Service—had “close links” with police Special Branches (Murphy et al., 2006, p. 36). Despite that, it noted the security service acknowledged the need to work at an even closer level with police. That closeness was needed not just in metropolitan London, but also in regional areas of the country (Andrew, 2009, p.
Deputy Assistant Commissioner Peter Clarke, then head of Counter Terrorism Command in the Metropolitan Police Service in London and national counter-terrorism coordinator (Dodd, 2007), confirmed the need for that closer relationship. In 2007, during a lecture, Clarke indicated progress had been made (Clarke, P., 2007). He stated there was “no doubt that the most important change in counter terrorism in the UK in recent years ha[d] been the development of the relationship between the police and the security service” (Clarke, P., 2007, para. 20).

In Australia, a review of the Australian Intelligence Community (AIC), completed in July 2004, acknowledged the “turning point” that 9/11 had been for the local intelligence community (Flood, 2004, pp. 39–40), and the major change that had occurred in the security environment as a result of both global terrorism and transnational crime (2004, p. 10). That view was undoubtedly reinforced for Australia by the loss of Australian lives in the 2002 Bali terrorist attacks (Flood, 2004, p. 10 & pp. 39–40; Pickering et al., 2008, p. 36). Flood, in his review of the AIC, characterised the terrorism threat as being both new in scale, as well as its methods and ambitions (2004, p. 11). He quoted one extremist, by way of example, who said: “We are not trying to negotiate with you, we are trying to destroy you” (2004, p. 11). Flood went on to say that the Australian Security Intelligence Organisation (ASIO) and the Australian Federal Police (AFP) enjoyed a particularly close relationship, in part helped by their joint working in 2000 on the preparations for the Sydney Olympics, and their work concerning the Bali bombings (Flood, 2004, p. 75). Despite those favourable views, he noted challenges remained, including the ability of intelligence and law enforcement agencies to manage the use of classified intelligence in court proceedings and the AFP’s desire for the intelligence collection agencies to raise the priority given to gathering intelligence on transnational crime (2004, pp. 75–76).

Elsewhere in Canada, two reviews into terrorism related events focused attention on the nexus between intelligence and law enforcement. The first review concerned the detention, deportation and alleged torture of a Canadian citizen in 2002 as a result of intelligence shared by the Royal Canadian Mounted Police with USA authorities (O’Connor, 2006a, p. 11). In 2004, the Canadian Government launched an inquiry into the events surrounding Maher Arar’s subsequent detention in Syria following his deportation from the USA. The factual events report prepared by Commissioner O’Connor detailed how inter-agency friction, lack of information sharing, poor coordination, and “mixed signals” between the Canadian Security Intelligence Service, Royal Canadian Mounted Police and other agencies had resulted in unverified security intelligence being shared inappropriately with United States agencies (2006, pp. 11–462). Those findings were further reinforced by the outcomes of a second Canadian review, published in 2010, into a much earlier terrorism event.

The second review inquired into the investigation of the mid-air destruction of Air India flight 182 in 1985, which, before the events of 9/11, “held the nefarious distinction of being the most deadly act of international terrorism in history (italics in the original) (Hoffman, 2010, p. 18). In his report concerning the Air India investigation the commissioner—Justice Major—delivered a number of findings, several of which touched again on the issue of intelligence and law enforcement engagement. Those findings centred on issues such as the challenge of sharing information in a timely and cooperative manner, duplication of efforts by intelligence and law enforcement agencies, excessive secrecy, the distinction between evidence
and intelligence, and the lack of “institutionalised co-ordination and direction in national security matters” (Major, 2010, pp. 1–7).

Arguably, terrorism events had opened the policy window for the countries just discussed. The result of the window opening was that detailed reviews were undertaken, which presented findings that had revealed common themes regarding inter-organisational relationships between the intelligence and law enforcement communities. For example, the need to improve the sharing and management of information, the need for new relationship structures to combat new threats, and the need for improved coordination between all of the agencies involved. But the question remained as to what that translated to at the strategic level, and how it impacted the wider security environment.

NEW PARADIGMS, NEW RESPONSES

The terrorism events occurring between 2001 and 2005 had driven awareness globally that the world’s security environment had changed in profound ways (Clark, H., 2001 & 2002a; Goff, P., 2001; Kean et al., 2004, pp. 326–328; Murphy et al., 2006, p. 40). But terrorism was just one manifestation of the increasing menace posed to countries by a variety of transnational crimes (Goldsmith, 2012, p. 278; Naim, 2003, p. 29; Roth, 2014, p. 7; Smith & Grabosky, 2012, pp. 247–264). Other threats, such as people trafficking, illicit drug distribution, weapons smuggling, counterfeit pharmaceuticals, illicit cyber activity, and child pornography were also being encountered, and while not new, it was the scale of their expansion driven by “advances in communication and transportation” (Roth, 2014, p. 7 citing Dandurand, Tkachuk, & Castle, 1998, p. 2) which increased concern regarding them (Ash, 2013, p. 2; Australian Crime Commission, 2013; Reichel & Albanese, 2014). The end result being the development of a “common list of threats” (Bigo, 2000, p. 174) by governments which further blurred and merged the difference between activities occurring outside and inside national borders (2000, p. 172).

Arguably, two important strategic themes emerged from those developments and, in particular, the increased global visibility of transnational criminality. Those themes, which called for old ways of doing business to be reconsidered, were:

- The appearance of new styles of threat that failed to acknowledge the established notions of borders and sovereignty. In extreme cases they were considered to “threaten the integrity of the state itself” (Goldsmith, 2012, p. 296), for example, in Colombia, Italy, and Mexico (Godson & Williams, 1998, pp. 67–68)², requiring a re-think of policy settings and responses (Archambault, 2010, pp. 89–90; Ash, 2013, p. 6; Karlsson, 2012, p. 38; Naim, 2003, pp. 34–35; Roth, 2014, p. 17); and
- Different and more effective inter-organisational relationships were identified as needed as the new threats impacted multiple agency mandates and responsibilities. Furthermore, the threats crossed—or blurred—the historic domestic-foreign divide around which traditional bureaucratic structures were based (Clark, H., 2004a; de

---

² Roth (2014, p. 17) disputed this concept and contended that it “ignores the fact that most illicit activity is accomplished in a clandestine manner that precludes the collection of data to support these fears.”
OPTIONS AND RESPONSES

The need existed to re-consider the inter-organisational relationships pertaining to national security. Bureaucrats were confronted with the challenge of determining how different arms of the state should work together in response to threats that crossed bureaucratic boundaries. What relationship options did they have to choose from and which fitted best for the variety of “wicked” security challenges confronting governments and agencies? To address that question recourse was had to literature from various disciplines including public administration, organisational theory and management.

Furthermore, of relevance to the above situation and question, it was contended, was the issue of a country’s capacity to respond, or put another way, its resources. Countries with large (or developed) economies and bureaucracies potentially had greater capacity to bring to bear on “wicked” security issues. In turn, it can be argued that smaller countries had fewer such resources to call upon. The countries discussed earlier—the USA, UK, Australia and Canada—which it are argued to have large and developed capacities, were calling for their national security agencies to be better connected, working in harmony, and focusing on the new style threats (Flood, 2004; Kean et al., 2004; Major, 2010; Murphy et al., 2006; O’Connor, 2006). However, the question concerning what countries with lesser capacities were doing with their more modest resources remained less clear.

From the Hague Centre for Strategic Studies, de Spiegeleire (2013) counselled that “small” countries should have an advantage if they act as “small” countries. He suggested they not try to replicate the actions of large countries. Unfortunately, de Spiegeleire did not expand on what criteria he used to define “small,” but at the time he was speaking about national security developments in the Netherlands. In endeavouring to explore de Spiegeleire’s thesis and determine which countries were in fact small and large it became evident that the division of countries into those two categories was too simplistic. For example, research revealed there was no universally agreed means of identifying what were small countries (and by default what were not) (Thorhallsson, 2006, p. 8), and that when small countries were discussed, they were often very small, for example, the island nations of the Pacific.

That conundrum led, as explained in the upcoming methodology chapter (see Chapter 3), to the determination that a more appropriate division of countries would be to group them into three relatively broad categories based on an amalgam of criteria collectively termed capacity, namely: large, intermediate, and small. That removed the truly small countries (in size and capacity) from consideration, and the truly large. However, when those that were left—the intermediate countries—were considered, the answer to the question concerning how they were behaving (or “responding” as de Spiegeleire termed it) still could not be found.

Therefore, this study sought to provide insight into how three of those intermediate capacity countries addressed inter-organisational relationships when it came to “wicked” security issues.
INTER-ORGANISATIONAL RELATIONSHIP TYPES

Over time, researchers and scholars have examined the various types of inter-organisational relationships occurring. Of particular interest to this study were the relationships arising when organisations tried to achieve an outcome which might prove more difficult—if not impossible—when tackled alone (Arnstein, 1969; Axelrod, 1984; Eppel, Gill, Lips, & Ryan, 2008; Himmelman, 2002; Huxham, 2003). The literature revealed several scholars who identified a hierarchy of organisational interactions, most commonly spanning cooperation, coordination, and collaboration (Axelrod, 1984; Cigler, 2001; Heavey & Murphy, 2012; Himmelman, 2002; Mattessich & Monsey, 1992; O’Flynn, 2009).

Common to all hierarchies of relationships, despite differing labels, was that each higher step required, or attracted, the need for additional inputs. Those inputs included the likelihood of increased compromise by the parties, and ultimately, acceptance of increased risk and loss of organisational “turf” (Cigler, 2001; Heavey & Murphy, 2012; Himmelman, 2002; Mattessich & Monsey, 1992). In their discussion of relationships, Cigler (2001, p. 74) and Himmelman (2002, p. 2) added a further level—to those commonly discussed—entitled “networking.” That level was described as involving the least degree of formality and input by those participating, and consequently sat below all other levels.

Mattessich and Monsey (1992) did not include networking in their typology, instead restricting the interactions to cooperation, coordination, and collaboration in that order (1992, p. 42). However, Eppel et al. (2008, p. 13) did include it, titling it “communication.” Eppel et al. posited that it was informal in nature and involved information sharing on an “as required” basis. The topic of networking has given rise to its own body of research and accompanying literature (Agranoff & McGuire, 2001; Cigler, 2001; Mandell, 2001). In at least one instance it was argued, “whereas the ‘3Cs’ are focused on relationships, networks are concerned with the structural arrangements between entities …” (Brown & Keast, 2003, p. 9).

From reviewing the literature on inter-organisational relationships, it became evident there were four commonly identified types. Those four types spanned a continuum ranging from the least formally connected and resource intensive, through to the most formally connected and resource intensive. For the purposes of the study, and drawing on the work of Cigler (2001, pp. 74–76), Eppel et al. (2008), Himmelman (2002, pp. 2–4), and Mattessich and Monsey (1992, p. 42), four distinct points on a RC were considered and situated in the following order:

- Networking;
- Cooperation;
- Coordination; and
- Collaboration.

Those four relationship types were given, for the purposes of this study, the collective title: NC₃.

Three other relationship descriptors were also assessed for possible inclusion in the typology. Co-production was considered. However, it was discarded due to it being a relationship focused on the interaction between service users (consumers) and service providers.
(departments or organisations) (McKenzie et al., 2008, p. 35; Ryan, 2012, p. 317). It was, therefore, outside the scope of this work that looked only at inter-organisational relationships.

Likewise, *partnership* was also considered. The term was often used interchangeably, or in conjunction, with collaboration (Andrews & Entwistle, 2010, pp. 679–680; Cigler, 2001, p. 75; Huxham, 2003, p. 402; Kanter, 1994, p. 97; Khan, 2003, p. 116). In the term’s dictionary definition, the reference to “shared expense, profit and loss,” (Oxford, 1989, p. 79) aligned with Himmelman’s depiction of collaboration. Himmelman (2002, p. 4) argued it involved a situation where “they share risk, responsibilities, and rewards.” Elsewhere, Mattessich and Monsey’s description of a collaboration involving “shared responsibility; mutual authority and accountability for successes” also corresponded. Therefore, it was determined partnership was sufficiently analogous with collaboration, or, according to Cigler (2001, pp. 74–75) all four points on the typology continuum, that it did not warrant a separate place.

Finally, another relationship descriptor that warranted examination was *unity of effort*. The term came to prominence through the findings of the 9/11 Commission (Kean et al., 2006, p. 416). The term was explored further by Severance (2005) in his PhD research. Severance determined that unity of effort should be viewed as a “fundamental organizational virtue that underlies or permeates the broader set of organizational efforts that are undertaken to achieve a desired outcome” (2005, p. 23). Thus, the outcome of considering unity of effort was that it also did not warrant inclusion.

Having confirmed the four distinct inter-organisational relationship forms (i.e. NC₃), the focus shifted to identifying what features each had, and how those features were either shared or principally linked to a particular NC₃ relationship type.

Firstly, using descriptions of inter-organisational relationships from the scholarly literature, it was possible to identify and assign features to a mind map (Buzan, 2002) representing each of the NC₃ relationship types. Table 2.1 shows the number of sources available, and how many actually contributed to construction of the four mind maps. The mind maps that resulted are contained in Appendix A. On completing construction of the mind maps, a review revealed they contained a variety of feature mention counts. For networking there were 67 identified features, for cooperation 37, coordination 36, and for collaboration 83. It was decided to reduce the total number of features requiring consideration to what consisted of the most often mentioned features in the literature, thus excluding features that had been mentioned only once or twice.

In deciding how to consolidate the feature numbers and thus reduce the volume, two mathematical calculations were explored. Firstly, the mode (O’Leary, 2010, p. 238; Prunkun, 2010, pp. 113–114) was considered to determine the most commonly occurring number of mentions features had for each relationship type. Secondly, the mean (O’Leary, 2010, p. 238; Prunkun, 2010, p. 112) was considered to determine the average number of mentions features had for each relationship type. Finally, because both the mode and mean were discovered to be small numbers that had limited impact in reducing the volume of features for consideration (i.e. the mode equalled one, and the mean equalled two or three), it was decided to also consider use of the median (O’Leary, 2010, p. 238; Prunkun, 2010, p. 113). That decision was further influenced by the discovery that the number of mentions for features in some mind maps had extreme numbers in their range. For example, in one relationship type the number of mentions per feature ranged from one to sixteen; however, there were no features with twelve to fifteen
mentions. Prunckun (2010, p. 113) recommended the use of the median when such circumstances were encountered.

When the median was calculated, it was found there was a different median for each relationship type. They ranged from three to six mentions. In applying the median, only features with the median—or higher—number of mentions would be considered and discussed further in the study. That reduced the data volume to a manageable level and ensured only features considered noteworthy by multiple authors were subject to consideration. Furthermore, in calculating and applying the median criteria, any feature with a counterpoint (i.e. one scholar identifies it as a feature, while another scholar discount it) had these subtracted from the number of mentions first. Then, only if the resulting number of mentions for the feature was at or above the median, was the feature considered further.

The outcome of applying the median criteria to the mind maps was: networking – 67 features reduced to eleven; cooperation – 37 features reduced to five; coordination – 36 features reduced to five; and finally, collaboration – 83 features reduced to eleven. The four reduced feature mind maps resulting from the process described are contained in Appendix B.

At the same time as the mind maps were being constructed, a spreadsheet was created that listed all the features appearing in all of the mind maps. The spreadsheet recorded the number of mentions each feature had, and any counterpoints related to it. By way of example, the results for the feature “resource sharing” are shown in Table 2.2.

Table 2.1. Sources for inter-organisational relationship type feature descriptions

<table>
<thead>
<tr>
<th>NC3 type</th>
<th>Potential sources of feature descriptions for each relationship type</th>
<th>Actual sources providing feature descriptions for each relationship type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networking</td>
<td>45</td>
<td>24</td>
</tr>
<tr>
<td>Cooperation</td>
<td>44</td>
<td>25</td>
</tr>
<tr>
<td>Coordination</td>
<td>46</td>
<td>20</td>
</tr>
<tr>
<td>Collaboration</td>
<td>46</td>
<td>26</td>
</tr>
</tbody>
</table>

---

3 A decision was made by the researcher to use five as the median number for networking. This was due to two numbers (five and six) being identified as the median during the calculation process.
The review of the consolidated feature descriptions firstly looked at the macro-level and sought to determine if any features were identified as relevant across the four relationship types. Once again, to be consistent, the median number for combined mentions was calculated across all the relationship types. The resulting median number was nine, therefore, only features with a total of nine or more mentions across all four types combined were considered. Eight features were found that met the criteria. They are shown in Table 2.3. The next step was to review the literature at the individual relationship type level, looking for any shared features. The process revealed a number of features shared by two or more relationship types. Those features are shown in Table 2.4. The final review of the literature sought to determine if there were features that were principally associated with only one relationship type. That revealed each type did in fact have features (or a feature in the case of cooperation) that met the median mentioned criteria, and were principally associated with just that one relationship type. Those features are shown in Table 2.5.

The eight features of relevance across all four relationship types (Table 2.3) led to the view forming—due to their cross-type noteworthiness—that those features were innate to the formation of inter-organisational relationships. It was argued that they represented the core rationale for why, when and how inter-organisational relationships developed.

### Table 2.2. “Resource sharing” mentions and counter points for each relationship type

<table>
<thead>
<tr>
<th>Feature</th>
<th>Networking</th>
<th>Cooperation</th>
<th>Coordination</th>
<th>Collaboration</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource sharing</td>
<td>16</td>
<td>1</td>
<td>5</td>
<td>2</td>
<td>8</td>
</tr>
</tbody>
</table>

No. of mentions found in the literature to the feature and its relevance to the NC3 relationship type
Table 2.4. Features shared by relationship types

<table>
<thead>
<tr>
<th>Feature</th>
<th>Networking</th>
<th>Cooperation</th>
<th>Coordination</th>
<th>Collaboration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informal (emergent)</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Formal (designed)</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Resource sharing</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Shared objectives/goals</td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Information/knowledge sharing</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Achieve what cannot be alone</td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Trust</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Governed without hierarchy</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 2.5. Features principally associated with only one relationship type

<table>
<thead>
<tr>
<th>Feature</th>
<th>Networking</th>
<th>Cooperation</th>
<th>Coordination</th>
<th>Collaboration</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 or more organisations</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contracting</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tackling “wicked” problems</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Can involve a central agency or lead agency</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reciprocity is expected between the parties</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lower level of intensity</td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Controller or work-regulator is used</td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Organisational turf is not given up</td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Collective action is undertaken</td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Some shared risk and reward</td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Good communication channels</td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Intense engagement between the parties</td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Greater time commitment is required for success</td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>
To elaborate on the core rationale concept (see Table 3.3), it was evident from the literature that inter-organisational relationships occurred when organisations needed to tackle difficult challenges and realised they could not resolve them alone (Axelsson & Axelsson, 2006, p. 80 citing Gray 1989; Foley, 2009, p. 442; Huxham, 2003, p. 403; McGuire, 2006, p. 35). For the public sector, those challenges were the “wicked” problems discussed earlier. In the private sector, the challenge was the need to continually innovate in the face of uncertainty and complexity in the environment (Farmakopoulou, 2002, p. 51; Muijs et al., 2010, p. 9). Organisations, therefore, entered relationships in order to share information and knowledge concerning the challenges they faced. Furthermore, they sought to garner access to resources they needed and did not have (Alter & Hage, 1993, p. 32; Cigler, 2001, p. 80; McGuire, 2006, p. 35). To accomplish the above, they needed to establish and maintain trust in their counterparts and contribute to some form of collective action.

The relationships themselves could develop from one of two quite distinct pathways. The first was the informal (emergent) path (Agranoff, 2006, p. 56; Cigler, 2001, p. 75; Mattessich & Monsey, 1992, p. 42). In those cases likeminded colleagues from different organisations recognised the challenges faced and came together to work on solutions (Provan, Fish, & Sydow, 2007, p. 482). While initially informal, those interactions could develop to the point where formality was required. Alternatively, the relationships could arise from the formal (designed) pathway (Brown & Keast, 2003, pp. 10–11; Himmelemann, 2002, p. 4; Mattessich & Monsey, 1992, p. 42) that involved organisations (or their overseers) deciding they needed to formally enter into a relationship with another (or others) to respond to particular challenges and to problem solve (Cigler, 2001, pp. 71–72; Provan & Kenis, 2007, p. 231).

Beyond the eight core features, Table 2.4 confirmed the existence of a number of features that were shared across two or more relationship types. Two features in Table 2.4 were shared across three relationship types. The first was one of the means by which relationships can be entered into: “formal (designed).” It was common to networking, coordination, and collaboration. One explanation for that arose from the view that inter-organisational relationships are very important to organisations (McGuire & Agranoff, 2011, p. 276). That importance arose through the need to commit resources either by way of shared material, knowledge, or staff time, and the effort required to make the relationship work. Therefore, it was contended that organisations found comfort in having a formal structure underpinning the value they assigned to their contribution and engagement.

The second three-way shared feature was “resource sharing”. It was common to networking, cooperation, and collaboration. Two possible explanations for that existed in the literature. The first theory described how a tightening of the economic environment saw resource scarcity occurring. That scarcity resulted in inter-organisational relationships forming to mitigate the threat (Thomson & Perry, 2006, p. 20). The second theory suggested that the narrowing of organisational mandates resulted in sharing. The narrowing of mandates resulted in greater specialisation and loss of the broader range of resources organisations were previously able to call upon from “in-house” sources (Andrews & Entwistle, 2010, p. 680; Knoben, Oerlemans, & Rutten, 2006, p. 390). That resource shrinkage resulted in inter-organisational relationships forming as a means of regaining access to a broader range of resources. The first theory outlined may have greatest applicability to the private sector, while
the second appeared more relevant to the public sector and the impacts of policies like New Public Management.

Additionally, Table 2.4 revealed that the feature “governed without hierarchy”—was relevant to networking and collaboration—and was also aligned with the feature “trust,” that alignment was considered noteworthy. After consideration, that alignment seemed a logical nexus, wherein, the absence of a hierarchically based power relationship resulted in a compensating formation of trust between the parties to a relationship.

A further observation from Table 2.4 concerned the formation of relationships. The relationship types networking and cooperation shared the feature “informal (emergent)”. While coordination and collaboration, shared “formal (designed).” Again, that seemed a logical situation given the relationships on the continuum were viewed as moving from an environment of loose organisational coupling (networking) towards tighter organisational coupling (collaboration) (Cigler, 2001, pp. 74–76). Therefore, the view formed that those relationship types closer to the loosely coupled end were likely to be from emergent arrangements, while those at the tighter end required formal design, although, that view did seem at odds with the concept of trust in collaborative relationships discussed earlier.

A further apparent contradiction to the above views was that networking shared the “formal (designed)” feature with coordination and collaboration (Table 2.5). That anomaly was discussed in the literature. It was argued that the “formal network” was the bureaucratic response to New Public Management’s specialisation and fragmentation of the public sector (Bollard et al., 2001, pp. 4–5; Doig, 2005, p. 423; Turrini, Cristofoli, Frosini, & Nasi, 2010, p. 528). Meanwhile, in the private sector, formal networking arose from the need to access resources to bridge the gap created by greater organisational specialisation. That relationship development occurred due to the need for continual innovation by private sector organisations in order to remain commercially viable (Muijs, West, & Ainscow, 2010, p. 6; Muller-Seitz, 2012, p. 428).

Finally, regarding the discussion of NC3 features, were those features identified as principally of relevance to one particular relationship type (Table 2.5). Those features were assessed to represent what the researchers considered were particularly noteworthy elements of each individual relationship type. Therefore, when viewed collectively and not individually, those features portrayed the essential differences between the four NC3 inter-organisational relationship types.

RELATIONSHIP CONTINUUM

Building on from identification of the four NC3 relationship types and their inherent features, consideration turned to how the researchers conceptualised the relationship between the four types. Several of the authors supported the concept of relationship types forming a set of steps (for example, see Cigler, 2001, pp. 71–72; Himmelman, 2002, pp. 2–4). The steps started with networking and concluded at collaboration. However, Smith and Wohlstetter (2006, pp. 251–252) sought to “challenge [that] assumption” and suggested that organisations determined the nature of their inter-organisational relationships “instead [on] context and individual circumstances.” They went on to assert “a new way to differentiate partnerships is needed –
one that assesses the different types of cooperation neutrally, so that participants may shape their partnerships based on their specific needs” (2006, pp. 251–252).

After reviewing the inter-organisational relationship literature, and deliberating on the contrasting views of a “hierarchical” continuum or a “context” and “circumstance” focused one, four interlinked concepts crystallised. The first concept related to the strong case the inter-organisational literature made for the existence of four relationship types (NC3). The four covered a range from the least formally connected and resource intensive, through to the most formally connected and resource intensive (Axelrod, 1984; Cigler, 2001; Heavey & Murphy, 2012; Himmelman, 2002; Mattessich & Monsey, 1992; O’Flynn, 2009). The concept viewed the four types as moving organisations from positions of autonomy in their activities towards situations where mergers with others were the likely outcome (for example, see Brown & Keast, 2003, p. 6 citing work by Cigler (2001), Hogue (1994), Leatz (1999), and Sziron et al. (2002)).

The second concept, expanding on the first, drew directly from the works of Cigler (2001, pp. 74–76), Himmelman (2002, pp. 2–4), and Mattessich and Monsey (1992, p. 42). The concept situated the four NC3 types on a RC, bounded at the ends by the states of autonomy and merger. In their work on relationships, Eppel et al. (2008, p. 13) also identified autonomy—termed by them “co-existence”—as occupying a similar continuum position. Thus, that concept expanded the original four inter-organisational relationship types to six, through the inclusion of autonomy and merger.

The third concept concerned how the continuum should be depicted. The literature, through use of the term hierarchy, suggested a stepped and somewhat linear view; however, the third concept proposed an alternative rotating dial format. That format envisaged the RC as a dial with six settings that were capable of selection by organisations when they encountered situations requiring them to adjust their inter-organisational relationship arrangements. The concept of a dial expanded on Smith and Wohlstetter’s (2006) argument. In their view, context and circumstances induced (or forced) an organisation to move from a default position of autonomy to a new relationship setting. The new setting would have to suit both the organisation’s needs and the change drivers it faced. The drivers could be a “focusing event” as described by Birkland (1997, p. 22), or a slower-paced policy, environmental or issue based impetus.

The fourth and final proposed concept was that organisations actually made three interlinked changes when they shifted relationship settings. The first change was relationship type focused, the second was relationship structure focused, and the final one was relationship extent focused. With respect to structure, the change involved a variety of options spread across the different RC settings. For cooperation, coordination, and collaboration, the two options were to enter either a dyadic (i.e. one to one) or networked (i.e. one to two or more) arrangement (Alter & Hage, 1993, p. 49; Muller-Seitz, 2012, pp. 428–429; Provan & Kenis, 2007, p. 231). While for the other three settings—autonomy, networking, and merger—only one structure option existed at each setting. For autonomy the option was to remain independent. At networking the option was to engage with two or more other organisations. And finally, at merger, the option was ceasing to exist in the current organisational state.

Having selected its relationship type and structure, the third change an organisation made when rotating the RC dials was deciding the extent (or intensity) to which it engaged with its new partner(s). Various authors have considered that issue and described it in different
ways (for example, see Brown & Keast, 2003; Mattessich & Monsey, 1992; Provan, Fish, & Sydow, 2007; O’Flynn, 2009). Axelsson & Axelsson (2006, p. 82) wrote of “limited” and “extensive” activity, while Muijs, West and Ainscow (2010, pp. 18–19) discussed “low,” “medium,” and “high” intensity interactions. Taking account of those earlier and contrasting views, extent within this study was considered to have two levels. The first level was strategic, where joint objectives and outcomes (or visions) were agreed and organisations adjusted operational activity to achieve those agreements (for example, see Axelsson & Axelsson, 2006, pp. 81–84; Brown & Keast, 2003, pp. 7–8; and Cigler, 2001, pp. 71–72). The second level was specific, involving focused or targeted engagement addressing particular issues, predominantly at the operational level, and impacting only a particular part (or parts) of the organisations (for example, see Axelsson & Axelsson, 2006, pp. 81–84; Brown & Keast 2003, p. 7; Cigler, 2001, pp. 74–75).

To further expand the concept of extent, and drawing on scholarly views, strategic extent of engagement was most likely seen when organisations elected to coordinate or collaborate with others. The information presented in Table 2.4 supported this view with “shared goals and objectives” identified as a shared feature between the coordination and collaboration relationship types. However, organisations could also elect to limit themselves to a specific extent of engagement when coordinating or collaborating, it depended on what they were trying to achieve. An example of the specific extent occurring within a collaborative context was the creation of multi-agency units to address a clearly defined issue. Multi-agency threat assessment units (or fusion centres) were an example of that practice (Persson, 2013, pp. 8–9; Wardlaw & Boughton, 2006, p. 140). However, the specific extent of engagement was the only option when organisations were networking or cooperating (Brown & Keast, 2003, p 7 citing Winer & Ray, 1994; Mattessich & Monsey, 1992, p. 42). That proposition was supported by the lower level of intensity involved with relationships at the loosely coupled end of the RC. That proposition was also consistent with the data revealing that networking and cooperation were about information and resource sharing, and not involving shared goals or objectives (see Table 2.4). When it came to autonomy, there was no engagement with others, so the issue of extent was moot, while with a merger only strategic extent of engagement occurred due to the nature of the activity and the outcome.

Figure 2.1 was developed to depict the three adjustments made when situations dictated a change in inter-organisational relationships. In the figure, if the relationship dial (left side of Figure 2.1) rotated clockwise, the structure arrangement dial (centre of Figure 2.1) and extent of engagement dial (right side of Figure 2.1) also rotated clockwise the same number of settings. Thus, when an organisation determined the need to make a relationship type change, the three dials depicted in the figure all rotated the same number of settings to the right to establish the new arrangements, and in some cases the choices that needed to be made.

Two examples of the RC dials concept being used arose from the terrorist attacks of 9/11. The attacks were arguably examples of what Birkland called a focusing event (1997, p. 22). In the USA, following inquiry into the events of 9/11, a decision was taken to merge twenty-two federal agencies to form the new Department of Homeland Security (Department of Homeland Security, n.d.; Whelan, 2012, p. 1). It can be anticipated that inter-organisational relationships were already in existence between the various agencies involved, however, the federal government determined the need to reconfigure those arrangements. So the government
“rotated the relationship type dial” to merger for all twenty-two agencies. As a result, the structure dial also moved to merger, and the extent of engagement dial shifted to strategic, and a new organisation was created.

A different inter-organisational relationship outcome was achieved from the same 9/11 events in the UK with formation of the Joint Terrorism Analysis Centre (JTAC) (Andrews, 2009, p. 817; Bamford, 2004, p. 744). In that case, the decision was taken by “around a dozen” organisations (Andrews, 2009, p. 817) to rotate the relationship dial to collaboration. The structure dial shifted to the choice of dyadic or networked, and since “around a dozen” agencies were involved in the multi-agency venture, networked was the structural choice made. And finally, the extent of engagement dial shifted to the option of a strategic or specific intensity of relationship. In that example, the specific extent was chosen as the new entity (JTAC) was focused, or as Davies (2004, p. 509) put it “custom fitted” to address a particular and well defined aspect of the agencies’ mandates, namely terrorism threat assessment (Bamford, 2004, p. 744). JTAC was not, it was argued, a strategic engagement due to the wider work of the contributors (their overall organisational “turf”) not being affected by the change (Bamford, 2004, pp. 744–745). The JTAC approach was subsequently replicated in a number of other countries (Walsh, 2011, pp. 110–111; Wardlaw & Boughton, 2006, p. 140; Whibley, 2013, p. 5).

While the earlier use of the phrase “rotate the relationship continuum dials” could be interpreted as trivialising the process that was not intended. Undoubtedly, before actions such as those described above were taken, serious discussion and debate was entered into between organisations. In such situations, governments may also seek to exercise policy leadership and steer (or encourage) organisations into the inter-organisational relationships they desire. For example, the “whole of government” and “joined-up working” of the 1990s and 2000s in Australia and New Zealand were, arguably, examples of that government leadership/steering processes in action (Bollard et al., 2001, pp. 4–5; Christensen & Lægreid, 2007, p. 1059; Paul, 2005, pp. 31–32).

Changes, such as the formation of a mega-department or development of a collaborative venture between agencies, undoubtedly come with a variety of structural, personnel and technical challenges (Svendsen, 2010, p. 308). However, the dial concept for the RC (Figure 2.1) and use of the phrase “rotating the dial” aimed to visually clarify an interlinked and complex set of concepts. It endeavoured to present the scholarly views that inter-agency relationships consisted of a finite range of choices that were capable of being selected by (or imposed on) agencies. Smith and Wohlstetter (2006, pp. 251–252) suggested that this allowed organisations to assess “the different types of cooperation neutrally.” On the continuum, depicted in Figure 2.1, no relationship type setting was necessarily superior to any other, and each setting offered a choice regarding the breadth and depth of engagement an organisation decided was necessary to achieve its desires, in the circumstances it faced.
Figure 2.1. Relationship Continuum Dials
CHAPTER 3 — METHODOLOGY

DATA GATHERING

Preparation for Case Study Selection

To gather data that enabled country comparison and ultimately to determine which countries to use in the case studies, the following “screening procedure” (Yin, 2009, p. 91) was used. Four “operational criteria” (2009, p. 91) were chosen to provide a comparative assessment across multiple variables. That enabled identification of countries with similar levels of what this study terms capacity, but avoided, however, searching for an elusive perfect alignment given the various differences between countries (i.e. geographic, economic, and demographic). The operational criteria, based on the traditional variables used for country comparisons (Thorhallsson, 2006, p. 27) were:

- Population: measured in millions of people;
- Economy size: measured by annual gross domestic product (GDP);
- Annual spend on national defence: measured as a percentage of GDP; and
- Territory size: measured in square kilometers (sq. km.).

Four global data sets were then accessed that had applicability to the chosen operational criteria. Two of the data sets were from the World Bank’s website, and two were from the World Atlas’s website (World Atlas, 2013; World Bank, 2013). The World Bank’s data sets provided Gross Domestic Product (GDP) figures for the year 2012, and the spend of GDP on national defence figures for the year 2011 (the most recent figures available at the time of inquiry). The World Atlas data sets provided the population of each country (as estimated as at 2013) and territory size data (as at September 2013). The four data sets provided a pool of 193 countries to analyse for population and territory size, 190 economies to analyse for annual gross domestic product (GDP) size, and 124 economies to analyse for spending on national defence.4

Case Study Data

To discover the relationship(s) occurring between the case study countries intelligence community (IC) and law enforcement community (LEC), sources were gathered from publicly available official records. The sources covered the expected types of relationship(s), using material from policymakers and central agencies5—accessed by searches of official websites (Mason, 2002, p. 103; May, 2001, pp. 178–179; Sheringham et al., 2012, p. 2), and, the relationship(s) actually delivered by intelligence and law enforcement communities.

---

4 By comparison, the United Nations had 193 member countries as at 2012 (Albanese, 2012, p. 11).
5 A central agency is an organisation in a country’s bureaucracy able to exert influence over the actions of other agencies in the bureaucracy. For example, in New Zealand such an agency was the Department of the Prime Minister and Cabinet. This agency’s influence arose because it provided direct advice to the prime minister, and exercised public sector leadership on behalf of the prime minister and the Cabinet.
For the expected relationship(s), key term searches narrowed the focus to material relevant to the research. That included use of the terms: transnational crime, national security, intelligence, and law enforcement (Birkland, 2004, p. 191; Sheringham et al., 2012, p. 2). The publications searched for included (Atkinson & Coffey, 1997, p. 46; May, 2001, pp. 178–179; Sheringham et al., 2012, p. 2; Weiss, 1972, p. 53):

- Speeches and media releases by leading policymakers, such as prime ministers and Cabinet members;
- Releases of strategy, policy, or position papers;
- Central agency pronouncements or papers; and
- Legislation covering the roles, functions and mandates of agencies within the intelligence and law enforcement communities.

Next, sources were gathered to provide data that determined the relationship(s) delivered by the IC and LEC through their engagements with each other. Once again, official websites were searched to locate agency records, or, as Perakyla (2005, p. 869) described them, quoting Silverman, “naturally occurring empirical material” (i.e. material that exists, and is unaffected by the activities of the researcher). The searches sought material published by both the IC and LEC, and which contained data concerning their interactions with each other. Such material formed part of the “chain of command” concept described by Hansen (2005, pp. 454–455). As such, it should show the implementation of government policy and the flow-on of policy through to operational activities. Records relevant to the research included a range of publications (Atkinson & Coffey, 1997, p. 46; Bochner, 2003, pp. 310–311; Mason, 2002, p. 52; May, 2001, pp. 178–179) such as:

- Reports to parliament, including departmental statements and annual reports (or their national equivalents) by intelligence and law enforcement agencies;
- Minutes or records of parliamentary committees with responsibilities for intelligence and law enforcement activity;
- Intelligence and law enforcement community chief executives’ speeches and media releases; and
- Findings of reviews: either specially commissioned or carried out by oversight entities with responsibility for the intelligence and/or law enforcement communities (e.g. Inspectors-General, independent review bodies, and Offices of the Ombudsman or their equivalents).

The extensive use made of official records, documents and websites was deliberate and aimed to provide ease of access to material for the study. At the same time, the sources addressed the issues of validity and reliability concerning the data being used (Brodeur, 2010, p. 186; May, 2001, pp. 184 & 188–189; Silverman, 2010, p. 275). For the results of the study to withstand scrutiny, it was determined that high degrees of validity and reliability needed to be maintained, particularly as the work relied on documentary sources (May, 2001, p. 176). As an additional means of buttressing the validity and neutrality of the case studies (O’Leary, 2010, p. 31), an independent review and commentary mechanism was included in the study’s methodology, as described in the upcoming data collation and analysis section.
**Case Study Comparison**

The data required to undertake the comparison process was produced during each of the case studies, as detailed in the earlier sections.

**DATA COLLATION AND ANALYSIS**

**Case Study Selection**

Following initial scanning of the contents of the four selected data sets, and in the absence of universally accepted methods of grouping countries for comparison (Thorhallsson, 2006, p. 8), it was decided to split the contents of the data sets into categories. To achieve categorisation, “stratifying” parameters (Yin, 2009, p. 92) were determined for each criterion, resulting in three capacity levels: large, intermediate, and small. The stratifying parameters were set in an effort to split the countries represented in the data sets into three relatively even numerical groups, although the results showed that an even split was not always achievable.

The stratifying parameters were:

- **Population:**
  - Large: more than 10 million people;
  - Intermediate: 3–10 million people; and
  - Small: less than 3 million people.

- **Annual GDP:**
  - Large: more than 500k million United States Dollars (USD) per year;
  - Intermediate: 100k–500k million USD per year; and
  - Small: less than 100k million USD per year

- **Percentage of annual GDP spent on national defence:**
  - Large: more than 2% spent per year;
  - Intermediate: 1–2% spent per year; and
  - Small: less than 1% spent per year.

- **Territory:**
  - Large: more than 500k sq. km.;
  - Intermediate: 100k–500k sq. km.; and
  - Small: less than 100k sq. km.

Once the data had had the three stratifying parameters applied to it, the country distribution results displayed in Table 3.1 were achieved.

A spreadsheet was then developed with a column for each of the four operational criteria. The four data sets were then examined to identify the countries meeting the intermediate capacity stratifying parameters. Those countries had their names recorded in alphabetical order in the relevant columns of the spreadsheet.

Next, the countries recorded in the spreadsheet were reviewed to identify those that met the parameters across all four operational criteria. The four criteria review revealed that only three countries met that standard, they were: Finland, New Zealand, and Norway (Table 3.2). To

---

6 Population size is often the sole criteria used to compare countries. For example, the World Bank identified small states as those with less than 1.5 million people.
ensure a suitably sized case study selection pool a second review was completed to identify countries that met any three of the four criteria. That second process identified 15 countries that met three of the four criteria (Table 3.3).

**Table 3.1. Country capacity parameters and distribution**

<table>
<thead>
<tr>
<th>Operational criteria</th>
<th>Sample size</th>
<th>Capacity parameters</th>
<th>Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Population (millions)</td>
<td>193 countries</td>
<td>Large (above 10m)</td>
<td>84 countries</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Intermediate (3m to 10m)</td>
<td>50 countries</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Small (less than 3m)</td>
<td>59 countries</td>
</tr>
<tr>
<td>GDP (millions of USD)</td>
<td>190 economies</td>
<td>Large (above 500k)</td>
<td>22 economies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Intermediate (100 to 500k)</td>
<td>40 economies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Small (less than 100k)</td>
<td>128 economies</td>
</tr>
<tr>
<td>GDP on national defence (%)</td>
<td>124 economies</td>
<td>Large (above 2%)</td>
<td>39 economies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Intermediate (1% to 2%)</td>
<td>65 economies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Small (less than 1%)</td>
<td>20 economies</td>
</tr>
<tr>
<td>Territory (sq. km)</td>
<td>193 countries</td>
<td>Large (above 500k)</td>
<td>51 countries</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Intermediate (100 to 500k)</td>
<td>56 countries</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Small (less than 100k)</td>
<td>86 countries</td>
</tr>
</tbody>
</table>

**Table 3.2. Countries meeting the intermediate parameters for all criteria**

<table>
<thead>
<tr>
<th>Operational criteria</th>
<th>Intermediate parameter</th>
<th>Finland</th>
<th>New Zealand</th>
<th>Norway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Population (millions)</td>
<td>3m to 10m</td>
<td>5,366,100</td>
<td>4,383,600</td>
<td>4,896,700</td>
</tr>
<tr>
<td>GDP (m of USD)</td>
<td>100k to 500k</td>
<td>250,024</td>
<td>139,768</td>
<td>499,667</td>
</tr>
<tr>
<td>GDP spent on national security (%)</td>
<td>1% to 2%</td>
<td>1.5</td>
<td>1.1</td>
<td>1.6</td>
</tr>
<tr>
<td>Territory (sq. km)</td>
<td>100k to 500k</td>
<td>337,030</td>
<td>268,680</td>
<td>324,220</td>
</tr>
</tbody>
</table>

Analysis of the parameters not met by the fifteen countries (Table 3.3), revealed Denmark was the only country with a territorial difference (being 57 per cent under the intermediate threshold). The country with the smallest percentage difference between the parameter settings and the country’s data was Sweden, which had a GDP five per cent above the upper intermediate threshold. Further analysis was then conducted on the remaining thirteen countries in Table 3.3. Those that had not met the GDP parameter (eight countries) ranged from 37 per cent to 93 per cent below the lower intermediate threshold. Because those GDP figures more closely aligned with the small capacity thresholds those eight countries were excluded from further consideration. Analysis of the population parameter data (five countries), revealed the range of variation to be 114 per cent to 1544 per cent above the upper intermediate threshold. Those population data, therefore, more closely aligned with the large capacity thresholds, thus those five countries were excluded from inclusion in the case study selection pool.
Table 3.3. Countries meeting the intermediate parameters for three criteria

<table>
<thead>
<tr>
<th>Country</th>
<th>Criterion not met (country’s actual data)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bangladesh</td>
<td>Population (164.425m)</td>
</tr>
<tr>
<td>Belarus</td>
<td>GDP (63,267k)</td>
</tr>
<tr>
<td>Benin</td>
<td>GDP (7,557k)</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>GDP (51,030k)</td>
</tr>
<tr>
<td>Congo, Rep.</td>
<td>GDP (17,870k)</td>
</tr>
<tr>
<td>Denmark</td>
<td>Territory (43,094 sq. km)</td>
</tr>
<tr>
<td>Honduras</td>
<td>GDP (17,967k)</td>
</tr>
<tr>
<td>Malaysia</td>
<td>Population (28.307m)</td>
</tr>
<tr>
<td>Paraguay</td>
<td>GDP (25,502k)</td>
</tr>
<tr>
<td>Philippines</td>
<td>Population (94.013m)</td>
</tr>
<tr>
<td>Poland</td>
<td>Population (38.167m)</td>
</tr>
<tr>
<td>Romania</td>
<td>Population (21.466m)</td>
</tr>
<tr>
<td>Sweden</td>
<td>GDP (525,742k)</td>
</tr>
<tr>
<td>Tajikistan</td>
<td>GDP (6,967k)</td>
</tr>
<tr>
<td>Turkmenistan</td>
<td>GDP (33,679k)</td>
</tr>
</tbody>
</table>

The above analysis left Denmark and Sweden in contention for addition to the selection pool. Denmark because the only parameter it had not met was territory size, which was considered the parameter with the least impact on capacity, and Sweden because it registered the smallest percentage difference regarding the parameter it had not met. It was decided, therefore, in the interests of having as big a selection pool as possible to include those two countries. The selection pool had, therefore, expanded to consist of five countries: Denmark, Finland, New Zealand, Norway, and Sweden (Table 3.4). Four of those countries were identifiable as Nordic and had either land borders with each other, or with another country. The fifth was an island nation situated in Oceania.

Table 3.4. Capacity data for countries in case study selection pool

<table>
<thead>
<tr>
<th>Operational criteria</th>
<th>Intermediate parameter</th>
<th>Denmark</th>
<th>Finland</th>
<th>New Zealand</th>
<th>Norway</th>
<th>Sweden</th>
</tr>
</thead>
<tbody>
<tr>
<td>Population</td>
<td>5 to 10m</td>
<td>5,540,241</td>
<td>5,366,100</td>
<td>4,383,600</td>
<td>4,896,700</td>
<td>9,366,092</td>
</tr>
<tr>
<td>GDP</td>
<td>100 to 500k</td>
<td>314,242</td>
<td>250,024</td>
<td>139,768</td>
<td>499,667</td>
<td>525,742</td>
</tr>
<tr>
<td>GDP defence</td>
<td>1 to 2%</td>
<td>1.5</td>
<td>1.5</td>
<td>1.1</td>
<td>1.6</td>
<td>1.3</td>
</tr>
<tr>
<td>Territory</td>
<td>100 to 500k</td>
<td>43,094</td>
<td>337,030</td>
<td>268,680</td>
<td>324,220</td>
<td>449,964</td>
</tr>
</tbody>
</table>

To make the final case study country choices, three additional selection criteria were drafted and applied to the process and countries in the pool:

- A desire to undertake multiple-case studies in an effort to gain the most robust findings from the study, thus adding strength to the findings (Yin, 2009, pp. 38–39);
- The need to make the number of case studies undertaken manageable—“doable”—by one researcher (O’Leary, 2010, p. 128); and
A desire to achieve as much geographic separation as possible between the countries chosen.

Those criteria resulted in three decisions being made. The first was to limit the case studies to three. That number was believed manageable by the researcher, while still providing for the desired degree of robustness in the research findings (O’Leary, 2010, p. 29; Yin, 2009, pp. 160–161). The second decision was that to achieve the geographic spread desired, New Zealand would be one of the case studies. That decision acknowledged the close proximity of the four Nordic countries to each other. New Zealand also presented two particular advantages. The first was that it was the researcher’s home country, and the second was that the researcher had experienced working in New Zealand’s law enforcement and national security communities. New Zealand therefore presented an ideal pilot case study opportunity (Yin, 2009, pp. 92–95) in preparation for the two studies that would follow.

The third and final decision concerned which two of the four remaining countries to select. After reflection on the geographic spread criteria, it was decided that only one of the three countries sharing a common land border (i.e. Finland, Norway, and Sweden) would be included. That automatically resulted in Denmark being selected. The final country selected, after considering all the criteria, was Finland. That decision was based on the fact it had achieved a four-criteria intermediate capacity fit during initial analysis (see Table 3.2), and because of the remaining Nordic states it was the furthest away from Denmark.

Case Studies General Overview

As previously mentioned, to aid in collation each source gathered was assigned a case study specific identifier establishing its relevance to one of the three studies for ease of retrieval purposes. Once assigned its identifier, each source was stored in an electronic repository to await analysis.

The analysis of sources employed qualitative content analysis (Bochner, 2003, pp. 310–311; May, 2001, p. 193; Prunckun, 2010, p. 24; Shek, Pietila, Graeser, & Aarva, 2011, p. 24), supported by quantitative analysis to provide additional context (O’Leary, 2010, pp. 127–131; Prunckun, 2010, p. 54). Due to terms describing relationship types being used interchangeably (Mattessich & Monsey, 1992, p. 42)—some might even say casually (O’Flynn, 2009, p. 112)—analysis of the context surrounding relationship descriptors and text, was necessary. The analysis process, therefore, involved multiple readings of the source documents. The first reading of a source was used to locate text containing relevant relationship data. Once the data was located, a second reading was undertaken to confirm identification of the relationship type being discussed, its associated structure (i.e. either dyadic or networked), and the extent of engagement being referred to, along with any relevant additional context surrounding the relationship (Hodson, 1999, p. 24; May, 2001, p. 196; Morris & Ecclesfield, 2011, p. 242; Richards & Morse, 2013, pp. 155–159; Shek et al., 2011, p. 24). A third and final reading was completed confirming the alignment of the data to the particular inter-organisational relationship type, structure and extent of engagement discerned in the second reading, this time using, as reference points, the mind maps and RC (Figure 2.1) developed during stage one of the study.

The process of multiple readings was supported by Hodson (1999, p. 49) as a means of “developing categories and sub categories” when dealing with documentary data. It enabled
the close matching of the data to the earlier identified and described relationship types. It also allowed for the “exploration and development of new categories”—possibly identifying as yet unconsidered relationship types—should the data have required this (Richards & Morse, 2013, pp. 155–159). Examples of the development of new categories as suggested by Richards and Morse are discussed later in the study.

The readings for each case study were completed in two tranches. The first involved reading sources from government (and central agencies if they were identifiable) with the purpose of discovering what type, or types, of inter-organisational relationships policymakers expected and supported. The second tranche examined sources from intelligence and law enforcement agencies and set out to discover what inter-organisational relationships they were delivering.

The supporting quantitative analysis consisted of applying charting techniques to examine the number of times different inter-organisational relationship types, structures, and extent of engagement were identified in the data from each tranche. The charting displayed, using percentages, the number of identifications occurring for each relationship type, structure and extent of engagement to show which predominated in each case study. Once charting was completed, the results enabled inferences to be reached concerning what governments’ wanted (i.e. expected) and what agencies were providing (i.e. delivering). The combination of the quantitative and qualitative results made it possible to form a view on how each case study country was shaping and managing its intelligence and law enforcement inter-organisational relationships.

Independent review and commentary on each draft case study was integrated into the process through the use of a panel of experts. The panel consisted of a person from each case study country with a professional background and experiences relevant to the topic of the study (Weiss, 1972, p. 41). As each case study neared completion, the experts were provided with the draft findings relevant to their country. They were asked to consider the draft findings, against the context of their own knowledge, to determine if they found them consistent with the environment they knew and experienced. If the findings were not consistent, feedback was requested on what was missing and where data could be found to further research and address the gap. If the expert suggested additional research, the review process was repeated for the resulting second set of draft findings. The recruitment letter to potential experts, setting out the process to be followed, has been reproduced at Appendix C. The use of a panel of experts also helped mitigate any researcher bias inadvertently brought to the work (O’Leary, 2010, p. 29 & 168; Weiss, 1972, p. 41). The panel process also confirmed the validity of the draft case study findings as representative of the phenomena being researched (Silverman, 2010, p. 275).

For the New Zealand case study the expert panel member was Mr R. Mark Evans OBE, a Deputy Chief Executive at New Zealand Police with responsibility for strategy. For the Danish case study, the expert panel member was Ms Kira Rønn PhD, who at the time was a strategic analyst at the National Center of Investigations within the Danish National Police. In respect of Finland, the expert consulted was Mr Stefan Aniszewski, a former Finnish government official and employee of Finnish Customs. At the time of his involvement with the case study, Mr Aniszewski worked in Brussels for a European-based United Nations organisation as a senior technical officer in the field of compliance and enforcement. Each
expert provided a set of responses concerning the case studies, and an indicative example from each has been provided at Appendix E.7

New Zealand Case Study

Data gathering involved searching official New Zealand Government websites for publicly available secondary sources. The websites included a site containing archived ministerial releases and departmental sites for agencies in the intelligence and law enforcement communities. The following list identifies all of the organisational websites visited:

- New Zealand Parliament (beehive.govt.nz);
- State Services Commission (ssc.govt.nz);
- Department of the Prime Minister and Cabinet (dpmc.govt.nz);
- New Zealand Security Intelligence Service (nzsis.govt.nz);
- Government Communications Security Bureau (gcsb.govt.nz);
- New Zealand Customs Service (customs.govt.nz);
- New Zealand Police (police.govt.nz); and
- Immigration New Zealand (mbie.govt.nz and dol.govt.nz).

The gathering process involved three methods. The first used keyword and term searches. Additional parameters were also applied consisting of: each year in the research period (2007–2012), and specific document types being sought, such as speeches, media releases, or other published resources. The words and terms searched were:

- Transnational crime;
- National security;
- Intelligence;
- Security intelligence;
- GCSB;
- National Assessments Bureau;
- Law enforcement;
- New Zealand Police;
- New Zealand Customs Service; and
- Immigration New Zealand.

As the searching progressed and sources were identified, additional terms or words were added or, in cases where results were not achieved, dropped. The additional searches included the words and terms:

- New Zealand Government;
- Strategy;
- Publications;
- Annual reports;
- Briefing to incoming minister;
- Evaluations and reviews;
- Policies;

7 Complete sets of responses from each expert are available upon request directed to the author.
• Statement of Intent;
• Strategies and plans;
• Guides and standards;
• Research; and
• Strategic outlook.

At the completion of that process, searches were made of the journals database provided by Charles Sturt University’s library. Again, parameters were set including keywords and terms that were used interchangeably and in various combinations. The interchanging was in an effort to identify the best possible array of potential sources. The words and terms used were:

• New Zealand (used for all combinations);
• Security;
• National security;
• Transnational crime;
• Organised crime;
• Transnational;
• Inter-organisational relationships;
• Intelligence;
• Law enforcement;
• Customs service;
• Immigration service;
• GCSB;
• NZSIS;
• Security Intelligence Service;
• Government Communications Security Bureau;
• Government agencies;
• Domestic;
• Police;
• Inter-organisational;
• Relationships;
• Immigration; and
• Customs.

The third and final gathering method involved selective sampling (O’Leary, 2010, p. 170; Trochim, 2006, para. 10) of references in sources already identified. That method resulted in targeted searches of specific websites, and some additional general searches. Examples of both approaches included:

• Organised and Financial Crime Agency, via a general Internet search;
• Intelligence agencies review, from the State Services Commission website; and
• Strengthening New Zealand’s Resistance to Organised Crime, from the Ministry of Justice website.

At the end of the gathering process, 5535 responses for words, terms and specific titles had been returned and reviewed. That resulted in 132 potential sources being identified and gathered for collation and review. As each potential source was retained it was assigned an
identifier consisting of the letters “NZ” and three numerals, starting with 001. Those identifiers enabled quick retrieval of the sources from the electronic storage system. The identifier was also included in any notes created about the sources, which again enabled quick retrieval. Subsequently, duplicate or invalid sources (i.e. sources inadvertently gathered twice or found to have been created outside the research time frame) were eliminated from the sample. That pruned the original 132 sources down to the 125 used to provide data for the case study.

To collate the source documents two electronic repositories were created. In the repositories three categories were used to store the sources. They were: government relationship expectations, intelligence community (IC) relationship delivery, and law enforcement community (LEC) relationship delivery. A set of sub-categories using the originating agencies names sat beneath the three principal categories. The unique identifiers referred to earlier were included in the title of each source to ensure it could be matched back to the research log that recorded the history of their collection. Table 3.5 shows the distribution of sources across the three categories.

Table 3.5. New Zealand case study source distribution

<table>
<thead>
<tr>
<th>Category</th>
<th>Source documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government relationship</td>
<td>48</td>
</tr>
<tr>
<td>expectations</td>
<td></td>
</tr>
<tr>
<td>IC relationship delivery</td>
<td>25</td>
</tr>
<tr>
<td>LEC relationship delivery</td>
<td>52</td>
</tr>
</tbody>
</table>

With source collation managed, the focus shifted to data and its collation. The quantitative and qualitative data from the sources were collated using a spreadsheet. The three categories outlined above were applied to compartmentalise the data according to its origin. Under the category headings, the sub-categories were again the names of the originating organisations.

The first category—government relationship expectations—enabled collation of data from sources created by government ministers or the three central agencies. That data identified the types of relationships sought and supported by the government and their close allies in the state sector leadership.

The second category—IC relationship delivery—allowed for the collation of data from sources created by intelligence agencies. In New Zealand, that consisted of the New

---

8 In the New Zealand state sector there were three agencies known as the “central agencies.” They were: the State Services Commission (SSC), the Treasury, and the Department of the Prime Minister and Cabinet (DPMC). Those agencies identified their role within the sector as “working together as a ‘Corporate Centre’ to lead a State sector that New Zealanders can trust, and that delivers better public services, including outstanding results and value for money” (Department of the Prime Minister and Cabinet, n.d. (c); Treasury, 2013, 19 Mar 2013). Two of the agencies featured prominently in the research. They were SSC and DPMC. DPMC’s role as a central agency included: “… convey[ing] Cabinet decisions to the relevant ministers and officials … DPMC also had a leadership role in relation to government themes and priorities, including conveying government priorities to officials.” (Treasury, 2013, 19 Mar 2013). While the SSC’s central agency role included “… ensure[ing] that State servants focus on addressing government priorities” (Treasury, 2013, 19 Mar 2013). Thus, the two agencies assisted ministers in ensuring the state sector delivered the government’s priorities and policies.
Zealand Security Intelligence Service (NZSIS), the Government Communications Security Bureau (GCSB), and units within the Department of the Prime Minister and Cabinet. The prime minister’s department contributed the National Assessments Bureau (NAB), Intelligence Coordination Group (ICG), and Security Risk Group (SRG) to the community. The third category—LEC relationship delivery—enabled collation of data from sources created by the New Zealand Police, New Zealand Customs Service, and Immigration New Zealand. All data records included the year in which the source document was created, the assigned unique identifier, and a brief title for the source document.

Table 3.6 provides a summary of the New Zealand agencies identified as relevant to the case study and their tasks.

Table 3.6. New Zealand agencies

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Agency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intelligence</td>
<td></td>
</tr>
<tr>
<td>Domestic</td>
<td>New Zealand Security Intelligence Service</td>
</tr>
<tr>
<td></td>
<td>(NZSIS)</td>
</tr>
<tr>
<td>Foreign</td>
<td></td>
</tr>
<tr>
<td>Signals</td>
<td>Government Communications Security Bureau</td>
</tr>
<tr>
<td></td>
<td>(GCSB)</td>
</tr>
<tr>
<td>Law enforcement</td>
<td></td>
</tr>
<tr>
<td>Border</td>
<td>New Zealand Customs Service (NZCS)</td>
</tr>
<tr>
<td>Immigration</td>
<td>Immigration New Zealand (INZ)</td>
</tr>
<tr>
<td>Domestic</td>
<td>New Zealand Police (NZP)</td>
</tr>
<tr>
<td>Transnational</td>
<td>Shared by all three agencies above depending</td>
</tr>
<tr>
<td></td>
<td>on the issue</td>
</tr>
</tbody>
</table>

At completion of source collation, the qualitative “content analysis” technique (May, 2001, p. 193; Prunckun, 2010, p. 24; Shek, Pietila, Graeser, & Aarva, 2011, p. 24) described above was used to locate the data. That process was supported by quantitative analysis of the data to provide context regarding the number of times the different types of relationships, structures, extent of engagements, and motivations were identified in the sources (O’Leary, 2010, pp. 127–131; Prunckun, 2010, p. 54). Qualitative analysis, with quantitative support, was chosen as it had the potential to add “richness” to the findings (O’Leary, 2010, pp. 262–263), while at the same time enabling “triangulation” of the results achieved (Prunckun, 2010, p. 54).

Content analysis involved subjecting each source to a “second reading” (Hodson, 1999, p. 49), with the first reading having been the initial scan of the source during gathering. The second reading was more intense and helped to determine conclusively what data the source contained about inter-organisational relationships between New Zealand’s intelligence and law enforcement agencies. During the reading, specific text in the sources was searched for. That text involved references to inter-organisational relationships related to transnational criminality, organised crime, or national security. Those three phrases were chosen as the first link directly to the research question. The second was included after identifying that in New Zealand the term “organised crime” was commonly used to describe transnational as well as domestic organised criminality. While the third phrase was included because transnational crime was deemed a national security issue in New Zealand’s security arrangements.
It was, therefore, determined that identification of relationships involving any one of those three phrases would provide data relevant to the research question.

When text about an inter-organisational relationship associated with transnational criminality, organised crime, or national security was encountered the type of relationship was identified and classified as either direct or interpreted data through consideration of both the descriptive word(s) used and the context surrounding the use of the word(s). For example, a direct classification signified that the text used to describe the relationship type aligned with the mind map features for that relationship type (e.g. use of the word cooperation and associated text aligned with the mind mapped features of a cooperative relationship). Alternatively, an interpreted classification signified one of two possible situations. The first was that the text used to describe a relationship type did not align to the relationship type indicated, and that an alternative relationship type had actually been described (e.g. use of the word cooperation, while the associated text actually aligned with the features of a coordination relationship). The second situation was when text about an inter-organisational relationship was encountered, but none of the relationship descriptor words were used in respect of it; therefore, the context had to be used to interpret what type of relationship the text was describing. The interpreted relationships were classified and recorded against the inter-organisational relationship types they aligned to most closely.

Through the process described above most data could be confirmed as pertaining to one particular inter-organisational relationship type; however, some data could only be narrowed to fitting two or three of the six relationship types. The inability to narrow all of the data to one relationship type was due to the common and shared features some relationship types enjoyed, as discussed earlier (see Tables 2.3 and 2.4). When a relationship type could not be narrowed to one particular type through review of the source context and mind maps, it was not recorded in the data spreadsheet. That non-recording avoided the danger of double counting single relationships identified in the data (i.e. counting an identification as both coordination and collaboration). That had the unfortunate affect of reducing the amount of data available for analysis; however, overall, it strengthened the validity of the data that was recorded. For examples of the process described, refer to Appendix C.

In the case of both classifications (direct or interpreted), each time a relationship was identified in a source it was assigned the value ‘1’. The values were then recorded in the data spreadsheet in either the direct or interpreted data columns, alongside the title of the source being reviewed. As sources often contained multiple relationship identifications, at the end of a source’s reading the totals for each classification were calculated and entered in the spreadsheet. At the same time, using the context surrounding the relationship identification, qualitative information was also located and recorded. That information included the structure involved with the relationship (i.e. dyadic or networked) and the identity of the community (or communities) involved (i.e. intelligence and/or law enforcement).

---

9 There were a total of 30 instances where a particular relationship type could not be defined. In the New Zealand case study there were eighteen instances, in the Danish study there were eight, and for Finland there were four.
To finalise the data collation from each source, a brief free-text descriptive comment, summarising the overall relationship context, was added to the spreadsheet. Those comments enabled particularly relevant sources to be identified for additional consideration during the qualitative analysis and discussion of results.

In all, 274 direct identifications of inter-organisational relationships were made from the source documents, alongside 454 interpreted identifications. Table 3.7 shows the distribution of the identifications across the three categories.

**Table 3.7. New Zealand case study data distribution**

<table>
<thead>
<tr>
<th>Category</th>
<th>Direct identifications</th>
<th>Interpreted identifications</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government expectations</td>
<td>112</td>
<td>115</td>
<td>227</td>
</tr>
<tr>
<td>IC delivery</td>
<td>83</td>
<td>161</td>
<td>244</td>
</tr>
<tr>
<td>LEC delivery</td>
<td>79</td>
<td>178</td>
<td>257</td>
</tr>
</tbody>
</table>

As outlined earlier, the second reading process commenced with three sets of data and information being recorded (i.e. relationship type, structure, and communities involved). However, halfway through the sources it became apparent two additional types of data were available from the sources. The first concerned what motivated the identified relationship. On examination, three sub-categories of motivation were determined from the scholarly literature and the studies sources. They were: legislation, encouragement (by government or some other influential actor), and voluntary (without coercion or encouragement from an outside party) (Doig, 2005, pp. 426–427; Muijs et al., 2010, p. 17; Murdoch, 2009). Of note, it was posited, that for encouraged or voluntary motivation to exist, legislation needed to permit—or at minimum not prohibit—inter-organisational relationships.\(^{10}\)

The second additional type of data identified was the extent of engagement occurring within relationships. Again, two sub-categories of engagement were determined. The first sub-

---

\(^{10}\) Research of legislation in New Zealand revealed that each agency—with the exception of the Department of Prime Minister and Cabinet—was the subject of primary legislation. Primary legislation set out the functions of the agency and the parameters within which it operated. Such legislation was also able to authorise or limit the extent to which agencies could interact with others. For example, New Zealand’s *Policing Act 2008*, acknowledged that police might need the cooperation of others (i.e. citizens, agencies or other bodies) to carryout their functions (*Policing Act 2008, s. 10(2) (NZL)*). While the *Government Communications Security Bureau Act 2003 (NZL)*, identified one of the bureau’s functions as “… co-operat[ing] with, or to provide advice and assistance to, the following for the purpose of facilitating the performance of their functions … the New Zealand Police … the New Zealand Security Intelligence Service” (*Government Communications Security Bureau Act 2003, s. 8C(1) (NZL)*). Some legislation was specific about why engagement was permitted to occur. For example, the NZSIS had a defined function of making recommendations to Immigration New Zealand concerning “matters to be decided under the Citizenship Act 1977 or the Immigration Act 2009, to the extent that those matter are relevant to security” (*New Zealand Security Intelligence Service Act 1969, s. 4(1)(bc) (NZL)*).
category related to situations where the relationship was dealing with specific issues or tasks that only affected particular parts of the organisations involved. While the second, related to situations involving a strategic relationship, which included shared goals and objectives, and affecting all or substantial parts of the organisations.

The realisation of the existence of those two additional types of data resulted in approximately half the sources being subjected to an additional reading process to capture the newly identified data. The remaining sources had that data recorded during their second reading.

On completion of the readings the resulting data set—labelled NZ1—that included all identified inter-organisational relationship data was reviewed. The review identified two distinct sub-sets of data within NZ1. They included a sub-set concerning relationships between intelligence and law enforcement organisations that were not clearly linked to transnational criminality, organised crime or national security, that sub-set was separated and labelled NZ2. The other sub-set of data encompassed relationships between intelligence and law enforcement organisations that were clearly linked to transnational criminality, organised crime, and national security, that sub-set was separated and labelled NZ3.

After yet further examination of the data sets, it was observed that some of the descriptive comments in NZ2 linked the relationships involved to:

- Border security, management or control;
- Threat awareness or reporting;
- Cyber-crime or threats;
- Immigration matters;
- Counter proliferation of technology capable of use in weapons of mass destruction;
- Counter terrorism and designation of terrorist organisations; and
- People smuggling.

Reflecting on that discovery and the links the material had with transnational criminality, organised crime and national security, it was determined that NZ3 would be expanded to include the data from the sources that had given rise to the above list. That decision ensured NZ3 was reflective of all data with a link to transnational criminality. Overall, it was contended, the decision would lead to more robust findings regarding the nub of the research question, namely, the inter-organisational relationships occurring that addressed the “wicked” issue of transnational criminality. Through the process detailed above, data set NZ3 established itself as being of the greatest relevance in addressing the research question concerning New Zealand.

To assist in analysing NZ3, and presenting the results, charts were employed (Prunckun, 2010, p. 128). A set of “donut” charts were prepared, using percentages that reflected the number of times each of the six relationship types were identified within the sources. The other data gleaned from the readings process, and recorded in NZ3, concerning structure, motivation and extent of engagement were also analysed and presented using the same style of charts. Once again the results were displayed as percentages representing the number of times each sub-element had been identified in the sources.

**Denmark Case Study**

Data gathering for the Danish case study also involved searching official government websites for publicly available secondary sources. The searching for the case study was undertaken in
two tranches. The first involved accessing and searching official Danish websites using the English language sections that most provided. The second tranche involved searches of the Danish language sections of the websites using Danish words and terms obtained through use of the online Google Translate (n.d.) software that translated English words and terms into Danish. The same software was then used to translate the Danish language search responses into English enabling responses of interest to be identified. The software was used again to translate the full responses of interest from Danish into English to help determine if they should be gathered as potential sources of data.

During the searches various Danish Government websites were visited, including:

- The Danish Prime Minister’s Office (stm.dk);
- The Ministry of Taxation (skat.dk);
- The Danish Security and Intelligence Service (pet.dk);
- The Ministry of Defence (fnn.dk);
- The Ministry of Economic Affairs and Interior (oim.dk);
- The Police (politi.dk);
- The Danish Parliament (thedanishparliament.dk);
- The Danish Immigration Service (nyidanmark.dk);
- The Danish Military Intelligence Service (fe-ddis.dk);
- The Justice Ministry (justitsministeriet.dk); and
- The Danish Emergency Management Agency (brs.dk).

Once again, keyword searches were used, incorporating English words and English words translated into Danish. When multi-year search results were returned, the parameters of the research period (2007–2012) were applied to reduce the volume of material needing review. The words and terms searched for were:

- DDIS (English language abbreviation for the Danish Military Intelligence Service);
- Politi (Danish word for police);
- Customs;
- PET (abbreviation for the Danish Security and Intelligence Service);
- Immigration;
- Prime Minister;
- Security;
- Crime;
- Enforcement;
- Inter-organisational;
- National security;
- Organised crime;
- Intelligence;
- Transnational;

11 Alternative translation software, the subscription based GramTrans dan2eng (http://gramtrans.com) was trialed during the translation process. However, the free online Google Translate software was found to be easier to use and just as effective in translating the responses. Therefore, Google Translate was used for all sources in both the Danish and Finnish case studies.
- Transnational crime;
- Arkiv (Danish word for archive);
- Arsrapport (Danish word for annual report);
- Samarbejde (Danish word for cooperation);
- Politiloven (Danish word for Policing Act);
- Publikationer (Danish word for publications);
- Opgaver (Danish word for tasks);
- Udlaendingeloven (Danish word for Aliens Act); and
- Efterretningstjeneste (Danish word for intelligence).

At the conclusion of that process, searches were made of the journals database provided through Charles Sturt University’s library. Again, parameters were set, which included keywords and terms that were used interchangeably and in various combinations. Those words and terms were:

- Danish/Denmark (both used for each search combination);
- National;
- Security;
- Transnational;
- Crime;
- Intelligence;
- Law;
- Enforcement;
- Police;
- Policing;
- Frontex (the name of the European Union external border agency);
- High policing;
- Relationships;
- Public sector;
- Organisational relationships; and
- Organisational behaviour.

The final gathering method used was selective sampling. The method involved targeted searches for quite specific documents or topics that had been identified through earlier search responses, or via sources that had been gathered using the previously described methods. Examples included:

- Danish Government action plan for the fight against terrorism;
- Danish police reform;
- Action plan;
- Et politi i forandring – et borgernaert politi (translation: A police in change – a citizen police);
- Prime minister’s speeches;
- Danish organised crime strategy; and
- A Denmark that stands together.
At the end of the gathering process, 4947 responses for words, terms and specific titles had been returned and reviewed. That resulted in 107 potential sources being identified and gathered for collation and review. As each potential source was retained it was assigned an identifier consisting of the letters “DK” and three numerals, starting with 001. The identifier was included in any notes created that pertained to the sources enabling quick retrieval. Subsequently, duplicate, invalid (i.e. gathered twice or outside the research time frame), and untranslatable sources (i.e. Danish language sources that were formatted in a way that prevented use of online translation software) were eliminated from the sample. That reduced the original 107 potential sources to the seventy-three used to provide data for the case study.

The Danish sources were collated in the same manner as the New Zealand ones had been. The Danish study also involved storage of the sources in two electronic repositories, with three categories being used to group the sources. The categories were once again: government relationship expectations, intelligence community (IC) relationship delivery, and law enforcement community (LEC) relationship delivery. The sub-categories within the three categories were again the names of the originating agencies. The unique identifiers described earlier were added to the title of each stored source to ensure they could be matched back to the research log that recorded the history of the sources’ collection. Table 3.8 shows the distribution of the 73 sources across the three categories.

Table 3.8. Denmark case study source distribution

<table>
<thead>
<tr>
<th>Category</th>
<th>Source documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government relationship expectations</td>
<td>24</td>
</tr>
<tr>
<td>IC relationship delivery</td>
<td>13</td>
</tr>
<tr>
<td>LEC relationship delivery</td>
<td>36</td>
</tr>
</tbody>
</table>

With source collation completed, the focus shifted to data collation. A spreadsheet was once again created enabling the collation of the qualitative and quantitative data used, and again, the three categories were applied within it to group the data. Under the category headings, the sub-categories were again the names of the originating organisations. All data recorded in the spreadsheet included the year in which the source documents were created, a brief source title, and the assigned unique identifier.

The first category—government relationship expectations—enabled collation of data from sources that recorded statements, speeches and media releases by government ministers. That data identified the types of relationships supported and sought by the Danish Government. Unlike the New Zealand case study, there was no evidence of the existence of prominent central agencies in the Danish bureaucracy, therefore all expectation data came directly from government ministers.

The second category—IC relationship delivery—allowed for the collation of data from sources created by Danish intelligence agencies. In Denmark the intelligence community consisted of the Danish Security and Intelligence Service (PET)12 and the Danish Military

12 For the Danish case study, the English language title was used for organisations, but the Danish acronym (or initials) was used in conjunction with it. So, for example, the Danish National Police’s
Intelligence Service (FE) (Weller, 2000, pp. 172–173; Danish Parliament, n.d., The Intelligence Services Committee). PET formed part of the Danish National Police, and a large part of the security service, including its leadership, were based in the national police headquarters building (Danish Security and Intelligence Service, 2010, p. 5). Despite its close relationship with the Danish National Police, the security service was considered a separate entity that reported directly to the Minister of Justice (2010, p. 5). Meanwhile, FE formed part of the Danish defence force organisation with distinct “independent authority” for foreign intelligence gathering, including signals intelligence (Danish Defence Intelligence Service, 2013, The service’s history). The military intelligence service reported directly to the Ministry of Defence and the Defence Minister (Ministry of Defence, n.d., Ministry of Defence organisation chart).

The final category—LEC relationship delivery—allowed for the collation of data from the Danish law enforcement community. The researcher determined that the community—for the purposes of the study—consisted of the Danish National Police, the State Prosecutors Office for Serious Economic Crime (SØK), the Danish Tax and Customs Administration (SKAT), and the Danish Immigration Service (DIS)—an agency under the Ministry of Justice. The rationale for that determination was that each of those agencies was deemed likely to have responsibility for activity related to transnational criminality. The research subsequently identified that in Denmark operational customs work at the border was undertaken by the Danish Police (Frontex, 2014, Denmark: Politi), while the bureaucratic functions concerning revenue assessment and gathering was housed, and operated, from within SKAT (Ministry of Taxation, n.d., The organisation of the Danish Tax Authorities). The Danish Police, in their border role, were also identified as responsible for passport control (Danish National Police, 2007, p. 28). Immigration activities at the border were similarly structured, with police providing the operational element, while the DIS delivered the bureaucratic and post-border assessment and settlement programmes pertaining to immigrants, visa activity, and issues associated with residency (Danish Immigration Service, n.d., The Danish Immigration Service).

Table 3.9 provides a summary of the Danish agencies identified as relevant to the case study and their tasks.

Once the source collation process was completed, a qualitative content analysis approach was embarked upon using essentially the same process as described in the New Zealand case study methodology. However, there were two notable differences to the method applied during the Danish case study. The first difference was that the content of each source was read in its entirety during the second reading process. That was considered necessary for two reasons. Firstly, the Danish use of the word ‘samarbejde’ which can mean both cooperation and collaboration. The wider context surrounding the use of that Danish word, therefore, assumed considerable importance in the case study to aid in identifying the type of inter-organisational relationship being referred too. The second reason for reading each source’s entire contents was, that unlike the New Zealand intelligence and law enforcement arrangements, the Danish domestic security service: Politiets Efterretningstjeneste (PET) appear in the work as: Danish Security and Intelligence Service, or PET.
arrangements were unfamiliar to the researcher. Therefore, full source review was found useful in providing a broader appreciation of Danish intelligence and law enforcement arrangements.

**Table 3.9. Danish agencies**

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Agency</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Intelligence</strong></td>
<td></td>
</tr>
<tr>
<td>Domestic</td>
<td>Danish Security and Intelligence Service (PET)</td>
</tr>
<tr>
<td>Foreign Signals</td>
<td>Danish Military Intelligence Service (FE)</td>
</tr>
<tr>
<td>Border</td>
<td>Danish National Police</td>
</tr>
<tr>
<td>Immigration</td>
<td>Danish Tax and Customs Administration (SKAT)</td>
</tr>
<tr>
<td>Domestic</td>
<td>Danish National Police</td>
</tr>
<tr>
<td>Transnational</td>
<td>Shared by all four agencies above depending on the issue</td>
</tr>
</tbody>
</table>

The second difference between the case studies was that Danish sources included documents translated into English by their Danish originators, as well as sources in their original Danish language format. For the sources in English, the context surrounding inter-organisational relationship text remained important. That was confirmed after it was established that the words cooperation and collaboration were used in translated sources in an apparently random manner, without necessarily making the English language distinction between them.

The random use of the English words came to light when two potential sources, one translated into English and the other in Danish, were identified as the same document. Comparison of segments of text involving use of the Danish word ‘samarbejde’ and the English words cooperation and collaboration confirmed the Danish word was translated into English as either cooperation or collaboration without apparent regard for the difference in meaning and associated context (for example, see use of the word ‘samarbejde’ in the Danish and English language versions of the Danish Security and Intelligence Service Report, 2010, p. 12).

That discovery meant the researcher’s interpretation of the type of inter-organisational relationship being written about, and described by the word ‘samarbejde’ in Danish language sources, and cooperation or collaboration in sources translated into English, assumed even greater importance and was central to the validity of the case study findings. The availability of the earlier created mind maps for the NC<sub>3</sub> relationship types, and the careful analysis of the features associated with each identified Danish relationship, enabled those interpretations to be completed with a high level of confidence.

Therefore, as with the New Zealand case study, when text describing an inter-organisational relationship associated with transnational criminality was encountered, the type of relationship was identified and classified as either a direct or interpreted item of data through
consideration of both the descriptive words used and the context surrounding the use. For example, a direct classification signified that the word and associated text used to describe the relationship type aligned with the mind map features for that relationship type, (e.g. use of the word ‘samarbejde’ in a Danish language source, or cooperation in a translated source), thus indicating an accurate description of the relationship. Alternatively, an interpreted classification signified that a word and text used to describe a relationship type did not align to the relationship type indicated, and that an alternative relationship type had actually being identified (e.g. use of the word ‘samarbejde’ or cooperation actually aligned with the features of a collaborative relationship type). Furthermore, if inter-organisational relationship text was identified that did not include the use of a relationship descriptor it was recorded as an interpreted classification for the relationship type that it most closely aligned too.

Through the above described process, the majority of Danish and English language data could be confirmed as pertaining to one particular identified inter-organisational relationship type; however, some could only be narrowed down to two or three of the four types (i.e. networking, cooperation, coordination, or collaboration). The inability to narrow all of the identified relationship data to one relationship type was due to the common and shared features some relationship types enjoyed, as discussed earlier. In those cases the data regarding the relationship was not entered into the spreadsheet used to capture the content analysis results. For examples of the process described, refer to Appendix C.

In the case of direct and interpreted classifications, each time a relationship type was identified it was assigned the value ‘1’. The values were subsequently totalled for each source and recorded in the Denmark case study spreadsheet in the data columns alongside the title of the source involved. At the same time, drawing on the context surrounding the identified relationship(s), additional data was also recorded. That data concerned: the structure involved with the relationship (i.e. dyadic or networked), the identity of the communities (or community) involved (i.e. intelligence and/or law enforcement, or other), the identified motivation for the relationship, and the extent of engagement pertaining to the relationship. The data record was completed with a short commentary summarising the source and its relevance to the study.

At the conclusion of that process, 121 direct relationship type identifications were confirmed from the sources, along with 84 interpreted identifications. Table 3.10 shows the distribution of the data across the three categories.

In a similar experience to that encountered with the New Zealand case study, the second reading process also resulted in greater understanding of Danish bureaucratic arrangements and the terminology used in connection with it. For example, “serious organised crime” was a phrase encountered that encompassed transnational crimes in its Danish usage (for example, see Danish Security and Intelligence Service, n.d. (b), About PET; and Danish National Police, 2009, p. 21), while “cross-border” was also a term used by the Danes when referring to transnational matters (for example, see Danish National Police, n.d. (b), p. 6).

Table 3.10. Denmark case study data distribution

<table>
<thead>
<tr>
<th>Category</th>
<th>Direct identifications</th>
<th>Interpreted identifications</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
On completion of the second readings the resulting data set—labelled DK1—was reviewed. As with the New Zealand study, the presence of a sub-set containing data about intelligence and law enforcement inter-organisational relationships related to transnational criminality was identified. That sub-set of data was separated and labelled DK2. The data from DK1 (for government relationship expectations only due to the limited number represented in DK2) and DK2 were analysed to determine the percentages for the number of times particular relationship types, structures, motivations and extent of engagement were identified across the sources. Those percentages were charted using the same process as described in the New Zealand case study methodology.

**Finland Case Study**

Data gathering for the Finnish case study again involved searching official government websites for publicly available secondary sources. The website searching identified that Finnish Government sites provided three language viewing options—Finnish, Swedish, and English—and that the sites’ published the majority of their content in each of those languages. Therefore, the majority of the sources gathered were in English and accessed using the websites’ English viewing option. However, not all source documents were translated into English, or could be located, using the English viewing option. As a result some searches were undertaken using the Finnish viewing option. Those searches used Finnish words and terms obtained through use of the online *Google Translate* (n.d.) software that translated English into Finnish. The same software was then used to translate the Finnish responses into English enabling responses of interest to be identified. The software was used again to translate the full responses of interest from Finnish into English to help determine if they should be gathered as potential sources of data.

During the searches various Finnish Government websites were visited, they included:

- Government of Finland (Valtioneuvosto.fi);
- The Prime Minister’s Office (vnk.fi);
- Police of Finland (poliisi.fi);
- Finnish Border Guard (raja.fi);
- Finnish Immigration Service (migri.fi);
- Finnish Customs (tulli.fi);
- Ministry of the Interior (intermin.fi);
- Ministry of Defence (defmin.fi);
- Finnish Security Intelligence Service (supo.fi);
- Security in Society (yhteiskunnanturvallisuus.fi); and
- Finlex (finlex.fi).\(^{13}\)

\(^{13}\) Online database of Finnish legislation operated by the Finnish Ministry of Justice.
Keyword searches were used, incorporating words in both English and Finnish as described above. When multi-year search results were returned, the parameters of the research period (2007–2012) were applied to reduce the volume of material needing review. The words and terms searched for included:

- Supo (the popular Finnish language abbreviation for the Finnish Security Intelligence Service);
- Immigration;
- Prime Minister;
- Security;
- Crime;
- Law enforcement;
- Inter-organisational;
- National security;
- Organised crime;
- Intelligence;
- Transnational;
- Transnational crime;
- Cross-border;
- Annual report;
- Publications;
- Terror*;
- Police;
- Policing;
- Customs;
- Signals;
- Archive;
- Viestikoelaitos (translation: message pilot plant);
- PTR (Finnish acronym for Police, Customs and Border Guard cooperation arrangements); and
- PCB (English version of the acronym PTR).

During the source gathering process, searches were also made of the journals database provided by Charles Sturt University’s library. Again, parameters were set and these included keywords and terms that were used interchangeably in various combinations. Those words and terms were:

- Finl*;
- Nation*;
- Secur*;
- Cross-border*;
- Military;
- Intell*;
- Intern*;
- Organ*;
- Polic*;
- Security;
- Intelligence; and
- Services.

The final gathering method used was selective sampling. The method involved targeted searches for specific subjects that had been identified during earlier searches. Examples included:

- Government program;
- Situation centre;
- Prevention of Financial Crime Management Group;
- National Cooperation Network for the Prevention of Violent Extremism;
- Cooperation Act;
- Police Act;
- Criminal Investigations Act;
- Coercive Measures Act;
- Border Guard Act; and
- Customs Act.

At the end of the gathering process, 3398 returns for keywords, terms and specific titles had been reviewed. That resulted in 145 potential sources being identified and gathered for collation and review. As each potential source was retained it was assigned an identifier consisting of the letters “FD” and three numerals, starting at 001. The identifier was also included in any notes created pertaining to the sources enabling quick retrieval. Subsequently, duplicate, invalid (i.e. gathered twice, or outside the research time frame), or untranslatable (i.e. Finnish language sources that were formatted in a way that prevented use of translation software) were eliminated from the sample. That reduced the original 145 potential sources to the 32 used to provide data for the case study.

The same collation processes were used for the Finnish sources as were applied to the New Zealand and Danish ones. That process also involved storage of sources in two electronic repositories, with three categories being used to group the sources. The categories were initially (see below for why that changed): government relationship expectations, intelligence community (IC) relationship delivery, and law enforcement community (LEC) relationship delivery. The sub-categories within the three categories were again the names of the originating agencies. The unique identifiers mentioned earlier were added to the title of each stored source to ensure they could be matched back to the research log that recorded the history of their collection. Table 3.11 shows the distribution of the 32 sources across the three categories.
Table 3.11. Finland case study source distribution

<table>
<thead>
<tr>
<th>Category</th>
<th>Source documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government relationship expectations</td>
<td>13</td>
</tr>
<tr>
<td>IC relationship delivery</td>
<td>5</td>
</tr>
<tr>
<td>LEC relationship delivery</td>
<td>14</td>
</tr>
</tbody>
</table>

With source collation completed, the focus shifted to data collation. Once again, a spreadsheet was created to enable the collation of the qualitative and quantitative data identified, and as previously, the three categories described above were applied to group the data. Under the category headings, the sub-categories were again the names of the originating organisations. All data recorded in the spreadsheet included: the year in which the source document was created, a brief source title, and the assigned unique identifier.

The first category—government relationship expectations—enabled collation of data from sources that recorded statements, speeches and media releases by government ministers. That data identified the types of relationships sought and supported by the Finnish Government. Unlike the New Zealand study, but as with the Danish one, there was no evidence of central agencies, therefore all expectation data came directly from government ministers.

The second category, as mentioned above, was to have been intelligence community relationship delivery, allowing for the collation of data from sources created by Finnish intelligence services. However, it became evident that Finnish intelligence sources were limited in number and related only to the domestic security service—the Finnish Security Intelligence Service (often referred to by its Finnish acronym: Supo). There was little publicly available data about Finnish foreign or signals intelligence organisations or activities, as commented upon by Teirilä (2015, pp. 226–227). The reason for that became evident through review of Holmström’s (2013, pp. 265–284) discussion—supported by Weller’s earlier work (2000, p. 172)—and Teirilä’s more contemporary description (2015, pp. 223–227), confirming that Finland did not have a dedicated civilian foreign intelligence service. The Finnish Security Intelligence Service (Supo)—with its “counterterrorism, counterespionage and security” authority (Holmström, 2013, p. 265)—did, however, maintain foreign intelligence links, in particular with other Nordic security services (2013, p. 267; Teirilä, 2015, p. 223), the European Union’s “Club de Berne,” and the club’s off-shoot the Counter Terrorist Group (Holmström, 2013, p. 274).

---

14 Intelligence activities and agencies are commonly categorised as: domestic (also known as security), foreign, military and signals (also known as Sigint) (Weller, 2000, p. 172). Under those four broad headings the responsibilities regarding domestic (security), foreign and signals intelligence can be summarised as: domestic (security)—protection and defence of the state, its people, interests and property (Cornall & Black, 2011, p. 6) mostly from within the country through programs to counter terrorism, espionage, and other forms of extremism; foreign—“intelligence about the capabilities, intentions or activities of people or organisations outside” a country (2011, p. 6); and signals—“intelligence … derived from the interception of foreign communications” (2011, p. 7). Also see Hoffman, 2010, p. 37, for a further description of the division of labour between intelligence and law enforcement.
What little information was available did confirm that within the Finnish military there was an intelligence capability housed in the Intelligence Division known as the Finnish Military Intelligence Centre (FINMIC) (Holmström, 2013, p. 265). Finnish military intelligence had responsibility for “… the strategic and operative early warning system and distribution of military intelligence analysis concerning situational awareness and threats. … including national and international cooperation … [and] counterintelligence where the armed forces are concerned” (Teirilä, 2015, pp. 226–227).

On the signals intelligence front, Holmström (2013, p. 265), Weller (2000, p. 172) and Teirilä (2015, p. 227) identified that the Finnish military maintained such a service, known as the Finnish Intelligence Research Establishment (FIRE) (Holmström, 2013, p. 265, Teirilä, 2015, p. 227). Very little information could be found regarding FIRE, however, the Finnish Minister of Defence had confirmed that the signals intelligence capability was for military purposes only (Halminen & Teivainen, 2014). Moreover, earlier in 2007, the Finnish Broadcasting Company (Yle) had reported about Finland’s signals intelligence activities, stating the Supreme Administrative Court had exempted the defence forces from having to disclose information about those activities (“Supreme Administrative Court, the military intelligence establishment does not need to provide even more general information”, 2007).

With regards to any interaction between the Finnish military or signals intelligence capabilities and law enforcement, once again only limited information could be found. In his work, Teirilä (2015, p 227), did mention cooperation between the two, but provided no details of what that entailed. Teirilä went on to state that FIRE was “Finland’s only SIGINT provider [and that] SUPO lacks this capability, but its chief has suggested that SUPO’s need for and right to SIGINT should be considered” (2015, p. 227). That statement, supported by media reporting concerning discussion within Finland of the need for Supo to have access to signals and cyber intelligence (Laine, 2014) led to the conclusion that during the time frame for this research no relationship existed between Finland’s FIRE and Supo.

Limited data and the matters outlined above were not the only factors regarding Finnish intelligence arrangements to impact the case study’s methodology. The security service it transpired was a national police unit within the Finnish Police (Holmström, 2013, p. 265). Furthermore, the security service’s legislative responsibilities were covered under the Act on Police Administration (Finnish Security Intelligence Service, n.d., p. 4). Therefore, unlike New

---

15 Media reporting from 2013 (Huhtanen & Teivainen, 2013) identified that Finland had no legislation covering the interception of “cyber intelligence”. In its report the Helsinki Times stated that a task force was to be established to look into the issue and to report back on what legislation was required and who should be tasked with the role. The police or the military were suggested as potential organisations to undertake the work. The article also confirmed that the Defence Force’s Finnish Intelligence Research Establishment undertook signals intelligence work for the military.

16 Research identified that in 2012 the Finnish Defence Forces embarked on a major restructuring exercise, which included reorganizing the intelligence functions. The implementation phase of that reorganization commenced at the end of Autumn 2013/beginning of Spring 2014. The reorganization saw the establishment of the Finnish Defence Forces Intelligence Agency, which included the old elements of the Finnish Military Intelligence Centre (FINMIC) and the Finnish Intelligence Research Establishment (FIRE) (Finnish Defence Forces, 2012). The only information found regarding the new entity confirmed its activities as “monitoring, analysis and reporting of the military strategic situation and the military situation of the neighbouring area.” (Finnish Defence Forces, 2014). No reference could be found to any links the new entity had with Finnish law enforcement or Supo.
Zealand with its civilian Security Intelligence Service, or Denmark with its Security and Intelligence Service—an element of the police, but with separate legislation and a growing individual identity—Finland’s security service was what could be described as a traditional Nordic security police organisation (Holmström, 2013, p. 269). Furthermore, there was little official indication that that state of affairs was likely to change (Ministry of the Interior, 2008, p. 59). However, Holmström identified (2013, p. 277) that the service was undergoing a gradual process of change that sought to move it from its traditional security police culture to one more akin to a modern security service (2013, p. 277), and the Finnish media in 2012 quoted the then head of Supo as supporting a change from a security police organisation to a more modern civilian security service with a foreign intelligence component (Finnish secret police chief urges civilian intelligence service, 18 December 2012).

As a result of determining that Finland had only one intelligence organisation about which useful data could be obtained, it was decided the term intelligence community (IC) would not be used for the case study. Instead, the Finnish case study used the category ‘Finnish intelligence’ to collate sources under and simply made reference to: Finnish intelligence, or the intelligence service.

The final category—LEC relationship delivery—allowed for the collation of data from Finland’s LEC. The researcher determined—for the purposes of the study—that the community consisted of the Finnish Police, Finnish Customs, Finnish Border Guard, and the Finnish Immigration Service. The rationale for that determination was again that each of those agencies was deemed likely to have responsibility for, or be involved in, activity related to transnational criminality. Subsequently, it was revealed that the immigration service’s activities at the border were delivered by police and border guard personnel, while the immigration service delivered bureaucratic functions, post-border assessment and settlement programs pertaining to immigrants and refugees, and matters relating to obtaining Finnish nationality (Finnish Immigration Service, 2011).

Table 3.12 provides a summary of the Finnish agencies identified as relevant to the case study and their tasks.

Once data collation process was completed, a qualitative content analysis approach was embarked upon using essentially the same process as described in the New Zealand case study methodology. Again, as with the Danish case study, there were two notable differences to the method applied from that used in the New Zealand study. The first difference was that the content of each source was read in its entirety during the second reading process. That was necessary for the same reasons that arose in the Danish study. Firstly, the Finnish word ‘yhteistyöta’ can mean both cooperation and collaboration. The wider context surrounding the use of that Finnish word, therefore, assumed importance in the case study to aid in identifying the actual inter-organisational relationship type being referred to. The second reason for reading each source’s entire contents was that the Finnish bureaucratic arrangements were unfamiliar to the researcher. Therefore, full source review was found useful to gain a broader appreciation of the Finnish environment, particularly the intelligence and law enforcement realm.
Table 3.12. Finnish agencies

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Agency</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Intelligence</strong></td>
<td></td>
</tr>
<tr>
<td>Domestic</td>
<td>Finnish Security Intelligence Service (Supo)</td>
</tr>
<tr>
<td>Foreign</td>
<td>—</td>
</tr>
<tr>
<td>Signals</td>
<td>Finnish Defence Forces via the Finnish Intelligence Research Establishment (FIRE) for military matters only</td>
</tr>
<tr>
<td><strong>Law enforcement</strong></td>
<td></td>
</tr>
<tr>
<td>Border</td>
<td>Finnish Customs (Tulli)</td>
</tr>
<tr>
<td></td>
<td>Finnish Border Guard</td>
</tr>
<tr>
<td>Immigration</td>
<td>Finnish Immigration Service (FIS)</td>
</tr>
<tr>
<td>Domestic</td>
<td>Finnish Police</td>
</tr>
<tr>
<td>Transnational</td>
<td>Shared by Supo, Tulli, Finnish Border Guard and Finnish Police depending on the issue</td>
</tr>
</tbody>
</table>

The second difference between the two case studies was that the Finnish study sources included documents translated into English by their Finnish creators, and some entirely in Finnish. For the sources in English, the context surrounding inter-organisational relationship mentions remained important as it was difficult to establish if the English words cooperation and collaboration were being used appropriately given the dual meaning of the Finnish word ‘yhteistyöta’. Dual meaning meant the researcher’s interpretation of the type of inter-organisational relationship being discussed and described by the word ‘yhteistyöta’ in Finnish language sources, and cooperation or collaboration in English language sources, was important and central to the validity of the case study. The availability of the mind maps for the four relationship types (i.e. networking, cooperation, coordination, and collaboration) and careful analysis of the features for each identified relationship enabled those interpretations to be completed with a high level of confidence.

Therefore, as was done in the New Zealand and Danish case studies, when text about an inter-organisational relationship associated with transnational criminality was encountered, the type of relationship was classified as either a direct or interpreted item of data through consideration of both the descriptive words used and the context surrounding the use. For example, a direct classification signified that the word used to describe the relationship type aligned with the mind map features for that relationship type, (e.g. use of the word ‘yhteistyöta’ in a Finnish language source, or cooperation in a translated source), thus indicating an appropriate use of the word. Alternatively, an interpreted classification signified that a word used to describe a relationship type did not align with the features of the relationship type indicated. Instead, an alternative relationship type had actually been described (e.g. use of the Finnish word ‘yhteistyöta’ or cooperation actually aligned with the features of a collaborative relationship type). Furthermore, if an inter-organisational relationship was described in a source without the use of a descriptor, it was also recorded as an interpreted classification for the relationship type it most closely aligned too.

Through the above described process, most Finnish and English language data could be confirmed as pertaining to one particular inter-organisational relationship type, however, some could only be narrowed to two or three of the four types. The inability to narrow all of
the data to one relationship type was due to the common and shared features some relationship types enjoyed, as discussed earlier. In those instances the data regarding the identified relationship was not recorded in the spreadsheet for subsequent analysis. For examples of the process described, refer to Appendix C.

In the case of both direct and interpreted classifications, each time a relationship type was identified in a source it was assigned the value ‘1’. The values were subsequently totalled for each source and recorded in the Finland case study spreadsheet in the data columns alongside the title of the source being reviewed. At the same time, using the context surrounding the identified relationship, additional data were also obtained. That data concerned: the structure involved with the relationship (i.e. dyadic or networked), the identity of the community or organisation involved (i.e. intelligence service and/or LEC, or other), the motivation for the relationship, and the extent of engagement within the relationship. The data records were again completed by short commentaries that summarised the sources and their relevance to the study.

In all, 88 direct relationship type identifications were recorded, along with 82 interpreted identifications. Table 3.13 shows the distribution of the data across the three categories.

Table 3.13. Finland case study data distribution

<table>
<thead>
<tr>
<th>Category</th>
<th>Direct identifications</th>
<th>Interpreted identifications</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government expectations</td>
<td>58</td>
<td>48</td>
<td>106</td>
</tr>
<tr>
<td>Intelligence delivery</td>
<td>2</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>LEC delivery</td>
<td>28</td>
<td>31</td>
<td>59</td>
</tr>
</tbody>
</table>

Similar to the experience encountered with the New Zealand and Danish case studies, the second reading process resulted in greater understanding of Finnish bureaucratic arrangements and terminology. For example, “organised and other serious crime” or “highly serious crimes” were phrases that encompassed transnational crimes in their Finnish use (for example, see Finnish Customs Service, 2009a, p. 12; and Finnish Police, 2012, p. 8), while, like the Danes, the Finns used the term “cross-border” when referring to transnational matters (for example, see Ministry of the Interior, 2008a, p. 13; and Prime Minister’s Office, 2009, p. 93).

On completion of the second readings the resulting data set—labelled FD1—was reviewed. As was the case with the earlier two studies, the review confirmed the presence of a sub-set of data relevant to intelligence and law enforcement inter-organisational relationships related to transnational criminality. That sub-set of data was separated and used to create the FD2 data set. The FD2 data was analysed to determine the percentages for the number of times different relationship types, structures, motivations, and extent of engagement were identified across the sources. That analysis resulted in a number of inferences being arrived at about the inter-organisational relationships that were expected and delivered in Finland. The same style of charts as were previously used, were adopted for the Finnish case study.
Case Study Comparison

Since the data had been collated and analysed separately during each of the case studies, at this point the three sets of findings were brought together for the purpose of making comparisons. The findings were placed in tables that displayed the identified: relationship type, structures, extent of engagement, and motivation from across each of the case studies. Analysis of those tables consisted of identifying and commenting on similarities and differences between the three countries. That process enabled the development of policy and practice benchmark findings that encapsulated the essence of how those three intermediate capacity countries approached inter-organisational relationships in addressing “wicked” issues like transnational criminality.

LIMITATIONS

This study was not without limitations. The first limitation to be discussed ultimately gave rise to the second; it was the issue of secrecy that surrounds intelligence communities. For a variety of reasons intelligence communities seek to keep secret their activities, methods, capabilities, and information sources (Brodeur, 2005, p. 801; Flood, 2004, pp. 75–76; Walsh, 2011, p. 30). Through the use of publicly available secondary sources the study aimed to overcome the secrecy challenge. Use of sources already released into the public domain by the respective intelligence communities (or associated parties), meant the study accessed data already sanctioned for public use. Therefore, the sources and data were highly unlikely to put at risk any activity, method, capability or information source that still required the cloak of secrecy.

The second limitation was reliance on open-source secondary data in the form of published documents. Through relying on that source of data, the researcher had no control over what was, or was not, included in the documents. That was an issue recognised in the scholarly literature regarding the use of such sources (Hodson, 1999, p. 71; May, 2001, p. 197). In order to mitigate the limitation multiple data sources for each element of the study were sought (Yin, 2009, p. 90). Those sources came from a variety of authorities and authors at various levels within the case study countries bureaucratic arrangements, and from beyond them. While that had the potential to (and did) expand the volume of data gathered for analysis, it increased the reliability of the data, and the resultant findings. As a consequence, it was posited, that overall the wider gathering helped to strengthen the validity of the findings.

The final limitation needing acknowledgement was the use made of secondary sources from Denmark and Finland, and the language challenges associated with them. It was not possible to be sure the sources gathered were a complete set of those potentially available. Through the use of English language website viewing options, a variety of word and term searches, and the use of translation software, every effort was made to obtain a comprehensive set of sources, and to capture their true meaning in the data. That having been said, some websites may not have been found, different keywords may have provided different results, the Danish and Finnish languages had words that encompassed multiple meanings in English, and translation software can only achieve so much in presenting the meaning of text from documents written in a language different to that used by the researcher. Every effort was made, however, to overcome those challenges as detailed above and in the methodology chapter. In particular, the expert panel members’ reviews were a key element of those efforts.
ETHICAL ISSUES

The data for the study came from open-source published documents. There was no data gathered directly from human subjects, or access made to sensitive or restricted data. The only interactions with people came in the form of the panel of experts who commented on the draft findings from each case study, and that was deemed to constitute a low ethical risk. However, to confirm that view an approval to proceed was sought from the Australian Graduate School of Policing and Security’s Human Research Ethics Committee (HREC). The approved was granted by the HREC on 1 April 2014, with a copy of that approval provided in Appendix C.
CHAPTER 4 — CASE STUDY RESULTS

OVERVIEW

The aim of the three case studies was to discover: (1) what intermediate capacity governments’
expected of their intelligence and law enforcement agencies with regards to inter-organisational relationships in addressing “wicked” issues, (2) what types of relationships the intelligence and law enforcement agencies were actually delivering, and (3) whether those relationships matched the government’s expectations.

The case studies were divided into three parts. The first presented and discussed the
analysis of data regarding governments’ expectations. The second part presented and
discussed the analysis of data regarding the delivery of relationships by the intelligence
communities (IC), while the third and final part did the same for the various law enforcement
communities (LEC). For each part the data was analysed using the two-tranche approach
detailed in the methodology section (i.e. the development of inferences after percentage based
analysis of the data, followed by qualitative discussion that provided examples which
illustrated (or challenged) the inferences arrived at earlier).

NEW ZEALAND

Government Relationship Expectations

The first tranche of analysis examined the government expectations data and established that
the data came from two quite distinct origins. The first was government ministers via
statements, speeches and documents, while the second was from central agency sources. As
outlined earlier in the work, New Zealand had three central agencies consisting of the State
Services Commission (SSC), the Department of the Prime Minister and Cabinet (DPMC), and
the Treasury. Because of that distinct split in the origin of expectation sources, it was decided
to analyse the data from each separately.

When the government data in data set NZ3 was reviewed it was noted that it
consisted of 32 identifications of inter-organisational relationships from seven sources. As
that was considered a small group of identifications to draw inferences from—in comparison
to the overall New Zealand data holding—consideration was given to resorting to use of one
of the other two data sets to determine the government’s perspective.

The consideration of which alternative data set to use identified that NZ2 recorded
51 identifications of inter-organisational relationships from eight sources, while NZ1
contained 99 identifications from 26 government sources. In light of that, it was decided data
set NZ1 was the most useful for determining what types of inter-organisational relationships
the government sought and encouraged between agencies during the research period.

The government expectations revealed by the data in NZ1 (Figure 4.1) were that
coordination was the most often identified relationship type, comprising 46 per cent (n=45).
That relationship type was followed by collaboration with 25 per cent (n=25), and cooperation
with sixteen per cent (n=16). Autonomy, networking, and merger had relatively small
amounts of data recorded for them (seven, one and five per cent respectively). That result led
to the inference that government expected a coordinated approach to policy implementation by operational agencies. In expecting that approach, the government was also shown to be comfortable with both cooperation and collaboration between agencies as elements of the coordinated delivery.

**Figure 4.1. New Zealand Government’s relationship expectations (n=99)**

Elsewhere, the central agency data in NZ3 (Figure 4.2) revealed 72 per cent of identified relationships concerned coordination (n=62), while fifteen per cent related to collaboration (n=13), and eight per cent to cooperation (n=7). Autonomy and merger had only small amounts of data recorded for them (four and one per cent respectively). There was no data for networking. The results obtained led to the inference that the government’s public sector leaders—the two central agencies that contributed to the data (i.e. Department of the Prime Minister and Cabinet and the State Services Commission)—focused on delivering the government’s coordination expectation, while also accommodating and supporting the use of collaboration and cooperation in its achievement.

Analysis then moved to consider the data regarding the structures and extents of engagement that the New Zealand Government expected. On the issue of structure, analysis revealed that the most commonly identified structure involved networked arrangements between three or more agencies. For the government (Figure 4.3) networked arrangements represented 63 per cent of identifications, while dyadic arrangements accounted for 27 per cent. For the central agencies (Figure 4.4), networks were 92 per cent of identified structures, with eight per cent being for dyadic arrangements. Those results led to an inference that government supported agencies formed networks when it came to entering into inter-organisational relationships. There remained, however, some room within the government’s expectations for simpler agency-to-agency relationships between organisations.
Figure 4.2. New Zealand central agencies relationship expectations (n=86)

![Chart showing relationship expectations with Collaboration at 72%, Coordination at 15%, Cooperation at 8%, Autonomy at 4%, and Merger at 1%]

Figure 4.3. New Zealand Government’s relationship structure expectations (n=30)

![Chart showing relationship structure expectations with Networked at 63%, Dyadic at 27%, and Autonomous at 10%]

Figure 4.4. New Zealand central agencies relationship structure expectations (n=12)

![Chart showing relationship structure expectations with Networked at 92%, and Dyadic at 8%]
Moving to the next relationship dimension, that concerning the extent of engagement, government expectations indicated a preference for specific engagement (focused on issues and tasks) with 68 per cent of those identified (Figure 4.5), while the central agencies (Figure 4.6) reversed that result with 72 per cent related to strategic engagement (focused on joint outcomes and goal creation, and policy development).

**Figure 4.5. New Zealand Government’s extent of engagement expectations (n=34)**

- Specific: 68%
- Strategic: 32%

**Figure 4.6. New Zealand central agencies extent of engagement expectations (n=18)**

- Specific: 28%
- Strategic: 72%

No data was sought or recorded concerning motivation when it came to government expectations. The reason for that was, as the policymaker, government was either legislating for relationships to happen, or encouraging them through the central agencies and their programs. In essence, government was, therefore, the principle driver of motivation.

Moving away from the inferences formed through percentage based analysis, and focusing instead on the qualitative nature of the data, two sources stood out for their relevance to the results and their importance to relationships in New Zealand. The first of those documents, produced in 2008 by the State Services Commission (SSC), was titled “Factors for Successful Coordination – A Framework to Help State Agencies Coordinate Effectively” (State Services Commission, 2008). The publication spelt out how coordination was
considered necessary to tackle “complex policy challenges” (2008, p. 6). The paper described coordination as an all-encompassing term that “… should be taken broadly and [was] not meant to exclude other forms of joint work. Quite the opposite: it [was] meant to cover the spectrum of joint activity from communication to collaboration” (2008, p. 7). In effect the SSC had told the New Zealand public service that coordination was viewed as a catch-all activity that encompassed all four of the NC3 relationship types identified earlier in the research. Further discussion of the SSC coordination document occurs later in this section.

The second important source, from a qualitative perspective, was a 2011 Department of the Prime Minister and Cabinet (DPMC) publication entitled “New Zealand’s National Security System” (Department of the Prime Minister and Cabinet, 2011b). Again, published by an influential central agency, the document outlined how national security issues were addressed in New Zealand. The document was found to apply a number of the terms and approaches outlined in the previously mentioned SSC document (State Services Commission, 2008), thus reinforcing the centrality of coordination. The National Security System publication will also be discussed further below.

As central agency publications, both the above documents stood out as important and authoritative markers for the public sector in New Zealand, including both the IC and LEC. The documents clearly articulated central agency thinking on how organisations were expected to interact with other agencies in their transaction of government business. Of additional relevance, given the timelines and drafting processes around policy documents in a bureaucracy, was that it was highly probable that the thinking and approaches they espoused pre-dated their actual publication. The two documents, it was contended, confirmed the strong expectation of a coordinated approach being taken to what were considered “complex policy challenges” (Gregory & Christensen, 2004, pp. 75–76; State Services Commission, 2008, p. 6) or, to build on Flemming and Wood’s (2006, p. 2) concept, “wicked” security issues.

In adopting the approach it had regarding the delivery of public service in New Zealand, the SSC had placed coordination at the heart of central agency efforts to move to what the SSC considered to be “the next generation of State Services” (State Services Commission, 2008, p. 5). One of six goals developed by the commission to achieve that transformation was the “Coordinated State Agencies Goal” (2008, p. 6). Through that goal the commission aimed to have agencies “committed to shared outcomes” and “work[ing] closely together and with partners to provide clear, joined-up responses to complex policy challenges” (2008, p. 6). In support of those two concepts, the SSC supported “share[d] decision-making … shar[ing] of information, knowledge and expertise … [and] pooling of resources …” (2008, p. 7).

In summing up its advice to the public sector, the SSC reminded agencies that “the challenges facing New Zealand [were] bigger than one agency can solve alone” (State Services Commission, 2008, p. 7). Furthermore, the commission contended that to be successful in applying the coordinated approach, factors such as leadership commitment, defined and agreed joint outcomes, and a mix of mandate, system and behaviour inputs were required to be in evidence (2008, p. 11). The Factors for Successful Coordination document was, therefore, quite unambiguous about what the commission, and by direct extension, the government, was requiring of state agencies.
Four examples of the SSC’s goals of “work[ing] closely together” and “shar[ing] information, knowledge and expertise …”, relevant to the study’s focus, were found in the data. While two of the examples (the Counter Proliferation Joint Section and the Combined Threat Assessment Group) pre-dated publication of the central agency documents referred to above, the four instances were considered indicative of the type of arrangements the central agencies sought, and which the scholarly literature discussed when considering collaborative ventures in public sectors (Axelsson & Axelsson, 2006, p. 82; Christensen & Lægreid, 2007, p. 1061). The examples, which also provided clarity concerning the types and nature of relationships formed between the IC and LEC in New Zealand, were:

- The Counter Proliferation Joint Section (CPJS) created to deal with countering the proliferation of dual use technologies associated with weapons of mass destruction. CPJS brought together the NZSIS, GCSB, NZ Customs Service and Immigration NZ in a co-located, collaborative, networked structure. The joint section was hosted by NZSIS (NZ Security Intelligence Service, 2011, p. 27);

- The Integrated Targeting and Operations Centre (ITOC) created and hosted by the Customs Service (Aniszewski, 2011, pp. 14–16; NZ Customs Service, 2012, p. 17). ITOC provided enhanced 24-hour border security capability. The centre’s staffing, co-located in a customs facility, came from: NZ Customs Service, Immigration NZ, Maritime NZ, NZ Police, Ministry of Primary Industries, and NZSIS (New Zealand Customs Service, 2011, pp. 28–29);

- The Combined Threat Assessment Group (CTAG) created to centralise analysis and reporting of terrorist and criminal threats to New Zealand’s interests. The group was formed in 2004 by: NZSIS, GCSB, NZ Police, NZ Customs Service, NZ Defence Force, and Maritime NZ (Clark, 2004b; Persson, 2013, pp. 35–36). It was originally hosted by the NZSIS, but later became part of that organisation in 2011; and

- The National Cyber Policy Office (NCPO) established in the Department of the Prime Minister and Cabinet in July 2012 (Ash, 2013, p. 5). The office had a “whole-of-government role, and was responsible, among other things, for implementation of [New Zealand’s] cyber security strategy” (2013, p. 5).

As already touched upon, each example was seen as operationalised evidence of the government’s expectations regarding cooperation, coordination and specifically collaboration (refer to Figures 4.1 and 4.2), using networked structures (refer to Figures 4.3 and 4.4), and focusing on a specific extent of engagement regarding issues and tasks (refer to Figures 4.5 and 4.6) as outlined in the inferences arrived at earlier. Additionally, the four examples listed also provided insight into the motivations for inter-organisational relationships in New Zealand. For example, the CPJS and ITOC were voluntary engagements, enabled by legislation that allowed for cooperative ventures (refer to Figures 4.10 and 4.14 below). While, CTAG and the NCPO were examples of encouraged engagement (refer to Figures 4.10 and 4.14 below), for instance, in the case of CTAG, its formation arose from a multi-agency process instigated by the Department of the Prime Minister and Cabinet and chaired by its then national security coordination unit, the Domestic and External Security Group (Author’s knowledge as the leader of the multi-agency process). While, in the case of the NCPO, the New Zealand Government approved the formation of the office as a further step toward
delivering the country’s cyber security strategy, with the cyber security risk having been identified as a “top priority” for the future (Department of the Prime Minister and Cabinet, 2012b, p. 4). No legislation (beyond that already in place) was enacted or changed to facilitate formation of any of the entities described above.

Moving on from the SSC’s efforts to embed coordination in the wider New Zealand public sector, a second central agency—the Department of the Prime Minister and Cabinet (DPMC)—aimed to do the same in the country’s national security sector. The department—responsible for overseeing national security coordination—identified through sources it published, that New Zealand’s Government perceived transnational criminality as one of a number of national security issues threatening the country’s “well-being” (Department of the Prime Minister and Cabinet, 2008, Operating Intentions: Contributing Outcome 4, para. 1; & 2011b, p. 26). Historically, in response to “wicked” security challenges, the New Zealand Government, through DPMC, had responded by putting in place a set of foundational bureaucratic arrangements to ensure inter-organisational coordination was achieved, as well as being desired.

The arrangements, that have been in place and operating—notwithstanding the politics of the day—for almost three decades (Department of the Prime Minister and Cabinet, 2011b, p. 7), were known as the Domestic and External Security Coordination (DESC) system. The DESC arrangements conjoined the bureaucracy and the government through the various mechanisms discussed below, and had at their head a Cabinet committee chaired by the prime minister (Hoadley, 2007, pp. 19–20; Murdoch, 2009, p. 4).

Situated immediately below the Cabinet committee, at the centre of the DESC system, was the Officials’ Committee for Domestic and External Security Coordination (ODESC) (Department of the Prime Minister and Cabinet, n.d. (b); Hoadley, 2007, pp. 19–20; Whibley, 2013, p. 5). It was through the ODESC, established with Cabinet authority in 1993 (New Zealand Security Intelligence Service Act 1969, s. 2(1) (NZL)), that ongoing policy oversight and issue-by-issue coordination was led and managed (Department of the Prime Minister and Cabinet, 2011b, p. 7). The officials’ committee, chaired by the chief executive of DPMC, had the chief executives from a broad range of government agencies sitting on it and/or its sub-committees (Department of the Prime Minister and Cabinet, 2010, p. 5, 2011b, pp. 23–24; Whibley, 2013, p. 5). That wide senior membership cohort was considered further evidence of the earlier revelation that the New Zealand Government favoured a networked structure (refer to Figures 4.3 and 4.4) underpinning its inter-organisational relationships.

The role of the ODESC was set out in detail in the 2011 National Security System document. In summary, the committee was described as being responsible for planning, preparation, response coordination, governance, and provision of insight into matters of national security, intelligence, and crisis management (Department of the Prime Minister and Cabinet, 2011b, p. 23). The structure of the arrangements and the ODESC’s role exemplified Gregory and Christensen’s (2004, pp. 75–76) depiction of New Zealand’s civil service. The two scholars described how the government set out to “… strengthen central coordination and control within the [state] sector …,” while Christensen and Lægreid identified the means used as “hierarchical strengthening of the centre” (2007, p. 1061).
The DESC system, and in particular the ODESC, placed a central agency in a primary coordination role, while, at the same time, reinforcing the prime minister’s departmental chief executive’s associated role as New Zealand’s National Security Advisor (Department of the Prime Minister and Cabinet, 2011, p. 12). The ODESC also played a role in bringing the chief executives of the IC and LEC (or their representatives) together as members of the committee, or as members of its various sub-committees (Department of the Prime Minister and Cabinet, n.d. (b); Whibley, 2013, p. 5). Of specific relevance to the study was the fact that one of those sub-committees was focused specifically on organised crime (New Zealand Police, 2011, pp. 36–37). The ODESC’s high-level membership and coordination role was consistent with Cigler’s view that the loss of autonomy associated with coordination meant “higher-level officials” would become involved in its oversight (Cigler, 2001, p. 76).

Beyond membership, the ODESC provided a further direct link between New Zealand’s IC and LEC via its Intelligence Governance sub-committee. That sub-committee was described as a “specialised” committee established at the direction of Cabinet to “… oversee governance and assurance in the intelligence community …” (Department of the Prime Minister and Cabinet, 2011b, p. 11). The sub-committee’s membership included the chief executives of the three central agencies and two “key customer” representatives, one of which was the commissioner of police (2011b, pp. 23–24). The sub-committee, therefore, clearly established a provider-customer relationship between intelligence and law enforcement agencies.

In contemplating the ODESC’s contribution towards the New Zealand Government’s inter-organisational relationship expectations, it was clear that the committee’s purpose and membership ensured coordination was driven, or put more eloquently “orchestrated” (Brown & Keast, 2003, p. 7; Muller-Seitz, 2012, p. 429 citing Dhanaraj & Parkhe), from the highest levels within the country’s national security agencies. That situation was entirely consistent with Axelsson & Axelsson’s (2006, pp. 79–80) proposition that coordination involved decisions being made at the top of structures for implementation by lower echelons. Furthermore, the positioning of the ODESC at the centre of the network, and engaging departmental chief executives as members, was indicative of the “all-channel” governance process described by Whelan, which he concluded was the most efficient form of network design (Whelan, 2012, pp. 43–45).

A final singular example of how central the ODESC was to New Zealand’s security arrangements was the fact that it was referred to in legislation covering the activities of the country’s security intelligence service. In section 4 of the New Zealand Security Intelligence Service Act 1969, the ODESC was named an entity the security service should report “any new area of potential relevance to security” to (New Zealand Security Intelligence Service Act 1969, s. 4(1)(d) (NZL)). That legislative reference, it was contended, signified the importance ascribed to the ODESC, and the networked structure it provided, as part of New Zealand’s response to “wicked” security issues, such as transnational criminality.

With the shape of the executive level of New Zealand’s response to “wicked” and complex issues outlined, the analysis shifted to focus on the year 2011. During that year central agency expectation and intelligence community delivery data concerning coordination and collaboration recorded notable spikes in volume. It was considered appropriate to explore
those phenomena further. Analysis identified 2011 as the year New Zealand published—for the first time—a Cabinet approved outline of how its national security system functioned and what it sought to achieve (Department of the Prime Minister and Cabinet, 2011b). The relevance of the document, referred to earlier and titled: “New Zealand’s National Security System”, in describing and understanding the New Zealand approach to complex or “wicked” issues during the period being studied was substantial.

The 2011 security system document did not prescribe a new approach—although it did include descriptions of “recent improvements to the system” (Department of the Prime Minister and Cabinet, 2011b, pp. 10–13)—instead it documented and confirmed the approach that had been in place for sometime, and that would, it can be inferred, continue to be applied into the future. In discussing the document and its contents, it was felt appropriate to also explore what came before it, as that was also considered relevant and influential regarding the evolution of New Zealand’s arrangements.

In May 2009, two years before the publication of the security system document, retired senior public servant Simon Murdoch was commissioned to review and report about the activities and structure of New Zealand’s intelligence agencies on behalf of the State Services Commission (Murdoch, 2009, p. 9). The terms of reference for the review pitched it as an exercise in achieving effectiveness and efficiency from the “core” intelligence agencies as a result of an earlier “line-by-line” financial review of them (2009, pp. 11–12). The Murdoch review, while carried out “under delegation from the State Services Commission,” was “at the invitation of the Prime Minister” in accordance with the provisions of the State Services Act 1988 (2009, p. 12).

Subsequently, in May 2010, the New Zealand Prime Minister confirmed he had commissioned the review, stating the reason was to “ensure the agencies keep pace with changes in the security environment, so we can better meet the security challenges we face” (Key, 2010). The prime minister’s interest and involvement was not exceptional given that the prime minister was the minister-in-charge of both the NZSIS and GCSB at that time. The prime minister’s department was also home to various national security units (i.e. the External Assessments Bureau and the Domestic and External Security Group) (Department of the Prime Minister and Cabinet, n.d. (c); Key, 2010).

Murdoch’s findings were reported back in October 2009 and the suggestions known to have been made (i.e. those contained in the released and unclassified version of the report) influenced proposals put to Cabinet in early 2010 (Key, 2010). Murdoch’s suggestions of relevance to the study included (Murdoch, 2009, pp. 5–9):

- Strengthening coordination, focus, and human resource flexibility across the intelligence community;
- Not merging the NZSIS and GCSB;
- Creating “a new interface with ‘homeland security’ agencies (i.e. border/law enforcement/organised crime) in future as part of a contemporary national security agenda”;
- “The senior officials’ committee, ODESC and the [Domestic and External Security] Committee of Cabinet to which it would normally report … should undertake NZIC governance at the systemic level … and operate through a DPMC based unit …”;

65
Consider giving a greater mandate and authority to the Intelligence Coordinator’s role, which was at that time a second-tier position in the Domestic and External Security Group, the national security unit inside DPMC; and

Further explore the UK practice of the Intelligence Coordinator being responsible for “… the ‘single intelligence account’, which I understand to mean that agency budget bids … are scrutinised from a collective angle …”.

Murdoch’s (2009) views fitted well with scholarly thinking on coordination and how it was achieved in security settings. That fit included: regulation of collective activity by a central actor, high-level official participation and structure, and improved interplay between intelligence and law enforcement (Alter & Hage, 1993, p. 93; Cigler, 2001, p.76; Foley, 2009, pp. 463–464). The Murdoch report and its outcomes were also examples of the encouraged motivation phenomena (refer to Figures 4.10 and 4.14) occurring in New Zealand. For example, the State Services Commission instigated the report, Cabinet approved the findings, and subsequently the Department of the Prime Minister and Cabinet oversaw implementation of them. It would have been clear to all agencies affected by the report that the implementation of the outcomes were being driven by very powerful forces. So, although all of the changes made were undertaken without a specific legislated mandate (or change to any existing legislation), the encouragement to go along with what was proposed by Cabinet and the central agencies would have been considerable.

In terms of moving forward on the report’s suggestions, in 2010 the Department of the Prime Minister and Cabinet acted by restructuring its national security staff in accordance with Murdoch’s suggestions. The department created two new business units by splitting and refocusing the Domestic and External Security Group. Thus, the Intelligence Coordination Group (ICG) and Security Risk Group (SRG) came into existence (Department of the Prime Minister and Cabinet, 2011c, Output Class 3: Intelligence Coordination and National Security Priorities, para. 3 and 10), while the External Assessments Bureau was renamed the National Assessments Bureau (NAB). The NAB was given a refocused mandate of developing a national assessments programme covering the domestic and foreign environments. The bureau’s new mandate also sought development of quality standards for the wider assessment community (Department of the Prime Minister and Cabinet, n.d. (d)). All of those moves were entirely consistent with what Hoadley described as the “orderly fashion” by which New Zealand goes about such changes in its bureaucratic arrangements (2007, p. 21).

With Cabinet’s approval of Murdoch’s recommendations, the ICG and SRG embarked on drafting the national security system document discussed above (Department of the Prime Minister and Cabinet, 2011c, Output Class 3 Service Performance: Intelligence Coordination Group, para. 4). The document set out “a comprehensive view of New Zealand’s national security interests and describe[d] how government agencies will work together to manage and respond …” (DPMC, 2011b, p. 3). Such language again reinforced what had been revealed elsewhere in the data regarding the importance accorded coordination and the use of networked structures working together on issues (refer to Figures 4.1 to 4.4 above, and 4.9 and 4.12 below). Furthermore, the document, with its Cabinet approval, was illustrative of the formalisation of coordination relationships, which various scholars discussed as a phenomena occurring commonly in such circumstances (Brown & Keast, 2003, pp. 10–11;

The author’s of the security system document used the opportunity of its drafting to define national security broadly, taking account of “globalisation and trans-boundary challenges” (Department of the Prime Minister and Cabinet, 2011b, p. 4), while risk management of national security issues was explained as involving “an ‘all-hazards’ basis … mean[ing] that all risks to national security whether internal or external, human or natural, [were] included …” (2011b, p. 5). Within that broad definition of national security, transnational criminal activity was identified as an issue (2011b, p. 19), and further reinforced in the document through references to: “cyber threats … illegal trafficking of people and harmful goods … promotion of violent extremist ideologies … trans-national criminal networks … [and] mass importation of drugs and other illicit commodities …” (2011b, pp. 18–19)—Bigo’s (2000, p. 174) common list of threats. While acknowledging that “straight forward issues” were—and should be—managed by responsible agencies, the document described how “major or complex situations” required central oversight, “lead agency” engagement, and “a group of government agencies” supporting the lead agency in its work (2011b, p. 6).

On the specific issue of intelligence and law enforcement community engagement, the national security system document was quite explicit. It stated:

Traditionally most intelligence agencies have operated relatively independently of each other and have not been well aligned with broader national security objectives. Work is underway to change this so that intelligence agencies have even closer relationships with, for example, law enforcement agencies such as Police, Customs and the Immigration Service. (Department of the Prime Minister and Cabinet, 2011b, p. 15)

Reinforcing the nature of those closer relationships, the national security system document later listed the lead and supporting agencies for various national security issues (Department of the Prime Minister and Cabinet, 2011b, pp. 25–26), for example (italics added):

- **International terrorism:**
  - Lead: Ministry of Foreign Affairs and Trade (MFAT)
  - Supporting agencies: *Police, DPMC, NZSIS, GCSB, NZDF*

- **Industrial espionage:**
  - Lead: Ministry of Economic Development (MED)
  - Supporting agencies: *Police, NZSIS, GCSB*

- **Illegal migrants/people trafficking:**
  - Lead: Department of Labour (DOL)—at that time parent agency for Immigration NZ
  - Supporting agencies: *Customs, Police, NZDF, MFAT, GCSB*

- **Trans-national crime:**
  - Lead: *Police*
  - Supporting agencies: *NZSIS, Customs, MFAT.*

In concluding discussion regarding lead and supporting agencies, it was considered important to highlight one particular aspect relevant to the study. In Annex D of the national security system document (Department of the Prime Minister and Cabinet, 2011b, pp. 25–26), terrorism and domestic extremism had NZSIS and NZ Police listed as joint-leads. The annex
contained only one other similar reference to joint-lead agency status out of the 62 issues it covered (2011b, p. 25). The joint-lead for terrorism and domestic extremism formally established an inter-organisational relationship between an intelligence agency and a law enforcement agency. Joint-leadership, while coordinative in respect of the supporting agencies was, it can be argued, moving NZSIS and New Zealand Police into a collaborative dyadic relationship on those two specific issues. That relationship was indicative of the quantitative data presented below in Figures 4.7 to 4.9 and 4.11 to 4.13.

In the New Zealand context, the joint-leadership arrangement made sense from the legal perspective, given the mandates of NZSIS and New Zealand Police. NZSIS was mandated by law (New Zealand Security Intelligence Service Act 1969, s. 4(1) (NZL)) to be the country’s internal security monitor, with security defined in the Service’s Act as including “prevention of any acts of terrorism” (New Zealand Security Intelligence Service Act 1969, s. 2 (NZL)); while simultaneously New Zealand Police were mandated to deliver, amongst other things, “crime prevention,” “law enforcement,” and “national security” (Policing Act 2008, s. 9 (NZL)). Terrorism in New Zealand, as elsewhere in the world (for example, see Husabø, 2013), was legislated as a crime and therefore, subject to law enforcement action (Greener-Barcham, 2002, pp. 511–512), including the use of coercive powers.

It appeared, therefore, that in an effort to reconcile those two overlapping legal mandates (and therefore, the overlap of “high policing” with “low policing” as described by Brodeur (1983 and 2007)), and to address the practical issue that NZSIS did not have the coercive or enforcement powers of New Zealand Police (New Zealand Security Intelligence Service Act 1969, s. 4(2) (NZL)), the joint-lead agency approach was adopted. In doing so, the national security system imbedded a collaborative arrangement between those two agencies when it came to preventing acts of terrorism or domestic extremism, both of which may involve elements of transnational criminality in the fluid twenty-first century security environment (O’Reilly & Ellison, 2006, pp. 645–646; Persson, 2013, p. 17). The joint approach closely mirrored similar “joined-up working” arrangements concerning terrorism occurring in the UK, which New Zealand—through its Five Eyes intelligence links—would have been familiar with (Bamford, 2004, p. 741; Brunatti, 2012, pp. 1–2; Her Majesty’s Government, 2006, p. 17 & 28; Manningham-Buller, 2007, pp. 44–45), and which appear to exist there for the same legal and practical reasons as those in New Zealand.

**Intelligence Community Relationships**

Moving the analysis from expectations and onto relationships actually delivered by agencies (refer to Table 3.6), the intelligence community (IC) was examined first. The IC data contained in NZ3 (n=228) revealed that cooperation accounted for 36 per cent (n=81) of identified relationships, followed by coordination with 31 per cent (n=71) and collaboration with 30 per cent (n=69) (Figure 4.7). Networking and merger represented two and one per cent of the identifications respectively, while there were none for autonomy or networking relationships. Those results were influenced by data from the Department of the Prime Minister and Cabinet, as the department was home to business units that were integral parts of the New Zealand IC (i.e. the National Assessments Bureau and the Intelligence Coordination Group). The business units were both active delivers of services, as well as propagators of the central agencies coordination mandate.
For example, 59 of the 71 relationships identified as coordination in the data originated from sources created by the Department of the Prime Minister and Cabinet intelligence community units. If that data were excluded from the analysis, the picture changed with the data from the NZSIS and GCSB identifying cooperation as the most often identified form of inter-organisational relationship (n=55 and n=6 respectively), followed by collaboration (n=36 and n=13 respectively). When the data were considered as a whole however, the analysis results produced the inference that the IC was delivering a blend of cooperative, coordinated and collaborative activity in accordance with the government’s expectations.

When it came to the structures employed to support those relationships (Figure 4.8), the analysis revealed that networked arrangements accounted for 70 per cent of identified structures, while dyadic connections accounted for 30 per cent. Again, the inference was drawn that the IC was in alignment with government expectations on this dimension.

**Figure 4.7. New Zealand’s Intelligence Community (IC) relationships (n=228)**

![Diagram showing relationship percentages]

The next dimension to be analysed was the extent of engagement involved in the relationships (Figure 4.9). That revealed that, while 55 per cent of engagement was at the specific (issue and task) level, 45 per cent was at the strategic level. That split was not in alignment with the previously identified government expectations. The outcome was assessed as again being reflective of the Department of the Prime Minister and Cabinet’s influence on the community, and its involvement of intelligence agencies in policy development and coordination activity (for example, see the discussion below of the ICG’s role and development of a joint intelligence community Statement of Intent).
The final dimension of IC relationships to be analysed was motivation. That process sought to assess the reasons why inter-organisational relationships were entered into. As outlined earlier, the reasons supporting a relationship forming can include legislation, encouragement, or a voluntary decision on the part of organisations.

The IC data (Figure 4.10) revealed encouragement accounted for 43 per cent of identified motivation, while legislation made up 38 per cent. Identified voluntary relationships accounted for nineteen per cent. The inference drawn from the result was that a mixture of encouraged and legislated motivations drove the majority of IC inter-organisational relationships, but that there remained room in the environment for the agencies to also show initiative in entering relationships where they were deemed appropriate.
Shifting from the development of quantitative inferences, and focusing on the qualitative content of the data, it was considered useful to again look at the description of the national security system, and in particular the effect the Intelligence Coordination Group (ICG) had on relationships. The ICG’s role statement confirmed the strategic extent of its mandate and the high profile tasks it was to undertake, which were: “Advis[ing] the prime minister on intelligence matters; provid[ing] priority setting, coordination and collaboration, resourcing, and evaluation of the New Zealand Intelligence Community (NZIC); and coordinat[ing] New Zealand’s international intelligence relationships” (Department of the Prime Minister and Cabinet, 2011c, Output Class 3: para. 10).

One of the first publicly acknowledged and notable achievements of the ICG’s strategic mandate was the production of a joint Statement of Intent (SoI) for the agencies making up the core New Zealand IC\textsuperscript{17} (New Zealand Security Intelligence Service, 2011, p. 7; Whibley, 2013, p. 4). The joint SoI document set out the priorities and performance criteria for the agencies—as a community—over the short to medium term (i.e. 2011 to 2016), while at the same time further imbedding the coordination, collaboration and networked expectations of the government across what was becoming known as the “intelligence sector” (Department of the Prime Minister and Cabinet, 2010, Statement of Intent: Operating Intentions: Objective Four; State Services Commission, 2013, p. 2).

Prior to the joint SoI, individual intelligence agencies prepared independent SoI documents. Although the statements no doubt referred to relationships with others, they were not formally linked. Indeed, the new joint approach confirmed, as Whibley reported, that the dictum for the new relationships within the intelligence community had shifted to “one community, many agencies” (Whibley, 2013, p. 2). The combined SoI process supported the earlier developed quantitative finding that the New Zealand Government desired a degree of strategic engagement between agencies, through a networked structural approach (refer to Figures 4.3 and 4.5). The “hierarchical strengthening” facilitated by the ICG, and the new role definition for the ICG leader (the Intelligence Coordinator), fitted Christensen and Lægreid’s

\textsuperscript{17} The core New Zealand intelligence community consisted of: NZSIS, GCSB and the National Assessments Bureau (Murdoch, 2009, p. 9).
description of New Zealand’s approach to public sector reform and its overarching “whole-of-government” agenda.

While still focusing on the newly articulated ‘community’ aspect of the intelligence agencies, data concerning the goals of that community were found despite the joint SoI not being publicly released. In the NZSIS’s 2011–2012 annual report, the director of security (i.e. the security service’s chief executive) identified them as including: “… using intelligence most effectively with agencies across government to achieve the best outcomes for New Zealand, for example in detecting people smuggling, combating organised crime, safeguarding national borders and protecting natural resources against illegal exploitation …” (New Zealand Security Intelligence Service, 2012, p. 5). Those goals, it was contended, provided further evidence of cooperative arrangements, networked structures, and both specific and strategic engagement on “wicked” issues linked to transnational criminality (refer to Figures 4.7 to 4.9 above, and 4.11 to 4.13 below).

Beyond the ICG, the Department of the Prime Minister and Cabinet’s other noteworthy contribution to intelligence relationships discussed in the national security system document was the National Assessments Bureau (NAB) (Department of the Prime Minister and Cabinet, 2011c, National Assessments Bureau). The bureau’s role was reported as comprising “coordination of assessments that draw on the resources of the whole of the NZIC,” while its director also chaired the National Assessments Committee (NAC) (2011c, National Assessments Bureau). The NAC was one of several standing sub-committees of the ODESC (Department of the Prime Minister and Cabinet, n.d. (d)). It was via the authority provided by chairing and coordinating the NAC that the bureau organised the preparation of assessments on national security issues, and endeavoured to set assessment standards for the wider assessment community. The NAC also provided the prime minister’s department with a further opportunity to engage with and influence agencies in the IC and the LEC, who were now being encouraged—in a change of approach commencing in 2007 (Department of the Prime Minister and Cabinet, 2008, Output Class 3: Service Performance18)—to provide assessments for consideration by the sub-committee (Department of the Prime Minister and Cabinet, 2012a, Statement of Service Performance: Output Class 3: NAB, para. 1; Department of the Prime Minister and Cabinet, n.d. (d)).

Both of the prime minister’s department units discussed above (ICG and NAB) were assessed as operational examples of the inferences developed earlier regarding the government’s coordination expectation. Both units coordinated a networked set of arrangements, engaging agencies at both the strategic and specific levels in their approaches to complex policy issues (refer to Figures 2.1 to 4.6). Furthermore, they were examples of the encouraged form of motivation evident in the New Zealand environment, as reflected in Figures 4.10 and 4.14, with neither relying on legislation to advance their agendas.

Having discussed how the coordination of security was orchestrated, it was not surprising to discover that the agencies delivering the arrangements were motivated to behave in the fashion revealed by the data. The data consistently showed the IC collaborating, coordinating, and cooperating (refer to Figure 4.7), within predominantly networked

18 Note: The External Assessments Bureau referred to in the cited reference was renamed the National Assessments Bureau in 2010.
structures (refer to Figure 4.9) or “cluster groups” (Hoadley, 2007, pp. 19–20), across the spectrum of extent (refer to Figure 4.8) (Dunne, M., 2008, pp. 24–25; Hoadley, 2007, pp. 19–20). Those findings were supported by Christensen and Lægreid’s contention that in New Zealand hierarchical strengthening resulted in a variety of mechanisms to achieve “…government units work[ing] better together” (2007, p. 1061).

Moving beyond the data provided by the national security system document, other evidence was found of efforts to increase the levels of inter-organisational engagement on “wicked” issues. For example, at the same time the security system document was being drafted, the intelligence community was experiencing restructuring specifically aimed at delivering greater degrees of coordination and collaboration (Ash, 2013, p. 6; Government Communications Security Bureau, 2011, pp. 1 & 4).

One particularly pivotal change impacting inter-organisational relationships came with the completion of GCSB’s new headquarters building. After high-level consideration a decision was taken to co-locate other elements of the intelligence and national security community in the building alongside the signals intelligence organisation (Department of the Prime Minister and Cabinet, 2010, p. 5). That decision moved the ICG, NAB, the Security Risk Group, and the Combined Threat Assessment Group from NZSIS where it was hosted into the new building (Department of the Prime Minister and Cabinet, 2010, p. 5; New Zealand Security Intelligence Service, 2011, p. 6). Subsequently, the co-location also included the newly established whole-of-government National Cyber Policy Office. The co-location arrangements were then further enhanced by the amalgamation of “back-office” functions across all of the entities resident in the building, which later, in 2013, also included the majority of the Wellington-based elements of the NZSIS (Brunatti, 2012, pp. 9–10; New Zealand Security Intelligence Service, 2013, pp. 6–7).

The co-location of the threat assessment group, a direct result of the Murdoch report recommending its alignment with the NAB (Murdoch, 2009, p. 7; NZ Security Intelligence Service, 2011, p. 6), highlighted a further interesting development in the New Zealand national security environment. Murdoch’s original co-location recommendation had subsequently been expanded upon by the decision to “integrate” the group fully into the NZSIS (New Zealand Security Intelligence Service, 2011, p. 6). That decision took CTAG from the status of a hosted, multi-agency, co-funded entity (Clark, 2004b), to being a business unit of its former host. Given the continued multi-agency nature of the threat assessment group’s staffing (Persson, 2013, pp. 35–36; Whibley, 2013, p. 5), that new arrangement was further evidence of strengthened intelligence community links with law enforcement.

On reflection, the co-location of the core intelligence agencies and the national security units from the prime minister’s department could be considered a form of enhanced collaboration. The entities retained their independent legislation, identities, functions and reporting lines (Brown & Keast, 2003, p. 7), but coalesced into a “sector” (State Services Commission, 2013, p. 2) dwelling side-by-side in one building, sharing a joint Statement of Intent, and submitting a combined budget to fund all parts of the newly structured “one community” (Whibley, 2013, p. 2).
Law Enforcement Community Relationships

Having analysed the intelligence community relationships, attention shifted to those of the law enforcement community (LEC). The approach used for the above sections was again applied, commencing with development of percentage-based inferences. On the topic of relationship types, the LEC data (n=103) revealed that collaboration accounted for 39 per cent of identified relationships (n=40) (Figure 4.11). Coordination followed with 36 per cent of identified relationships (n=37). Finally, cooperation represented 21 per cent (n=22), while autonomy and networking shared a minor number of identifications, and there were no data for merger. The inference to be drawn from those results was that the LEC was delivering relationships that aligned with the government’s expectations, but with slightly greater emphasis on collaboration and coordination than their intelligence counterparts.

Moving on from the type of relationships to the structures supporting them, analysis revealed an emphasis towards multi-agency arrangements with 76 per cent of identified structures involving networks. Dyadic arrangements accounted for 14 per cent of identified structures, while autonomy represented 10 per cent (Figure 4.12). Again, the inference drawn was that the LEC were delivering structures which aligned with the government’s wishes and which also aligned with the approach being taken by the intelligence community.

Figure 4.11. New Zealand’s Law Enforcement Community (LEC) relationships (n=103)
The next dimension to be analysed was the extent of engagement occurring within LEC relationships. Figure 4.13 showed that, as with the intelligence community, the split between strategic and specific focuses was 45 per cent and 55 per cent respectively. The inference formed was that the LEC was again in alignment with the government’s expectations.

Finally, for that tranche of analysis concerning the LEC, Figure 4.14 revealed that the motivations for entering into relationships encompassed all three types. Encouragement was the most identified form with 40 per cent. That was followed by legislation with 31 per cent and voluntary with 29 per cent of identifications. The results were similar to those of the intelligence community. That outcome reinforced the view arrived at regarding the IC, which was, that while encouragement and legislation drove the majority of inter-organisational relationships, voluntary engagement was also a live option and was being used. That led to the inference that organisations within the intelligence and law enforcement communities were cognisant of the government’s expectations and were prepared to act on them of their own volition when appropriate.
Approaching the LEC data from the qualitative perspective, once again the influence of central agencies, and in particular the Department of the Prime Minister and Cabinet, was evident. For the LEC the link was via the Security Risk Group (SRG), the sibling of the intelligence community’s ICG. The SRG was created to interact directly with operational agencies and law enforcement organisations with security responsibilities (Department of the Prime Minister and Cabinet, 2011b, p. 27). The SRG’s task was to drive coordination on national security issues and to work with agencies that delivered operational responses (2011b, p. 27). The group’s role was defined as:

Deal[ing] with national security threats that affect[ed] New Zealand and its interests, both onshore and offshore; coordinat[ing] the activities of central government agencies in preparing for and responding to security crises, emergencies and natural disasters; and advis[ing] the prime minister on intelligence and security matters. (DPMC, n.d. (c))

The SRG, with a different, but complementary, mandate to the Intelligence Coordination Group, was clearly targeted at preparation and response activities. At the same time the SRG was aiming to achieve the government’s desired outcome of coordination. Through its role and activities, the SRG provided central agencies with a mechanism by which to coordinate and influence the national security activities of the LEC. In doing so however, it carefully avoided impinging on the tricky issue of operational independence associated with law enforcement (for example, see Brodeur, 2010, pp. 223–224), a sensitive topic when dealing with the New Zealand Police (see Policing Act 2008, s. 16(2) (NZL)).

Elsewhere in the law enforcement data, two sources detailing initiatives to confront transnational criminality provided evidence of the community operationalising the government’s desire for coordination and collaboration through “work[ing] closely together and with partners to provide clear, joined-up responses to complex policy challenges” (State Services Commission, 2008, p. 6). The first initiative involved delivery of a whole-of-government Organised Crime Strategy (King, 2007, 2008; Ministry of Justice, 2008). The strategy described an intelligence-led approach to tackling a wide-ranging array of organised criminal activities (Ministry of Justice, 2008, pp. 1–2). The strategy was closely tied to the second initiative, the establishment in July 2008 of a national organised crime agency to be
known as the Organised and Financial Crime Agency New Zealand (OFCANZ) (King, 2008; Ministry of Justice, 2008, p. 4). While the strategy was identified as a coordinating mechanism focused on whole-of-government action (Ministry of Justice, 2008, p. 2; New Zealand Police, 2008, p. 16), OFCANZ’s design was two-fold. Firstly, the agency was to support the strategy’s whole-of-government coordinated approach to organised crime, and secondly it was to be a collaborative, collective-action catalyst for operations against organised crime, including transnational crime (Ministry of Justice, 2008, pp. 4–6; New Zealand Police, 2011, p. 36). Both the strategy and new crime agency were to be overseen by the ODESC (King, 2007, 2008).

At the same time as the introduction of the organised crime strategy and new crime agency, New Zealand Police were separately undertaking a fundamental restructuring and repositioning of their in-house intelligence arrangements (Walsh, 2011, p. 118). Starting in 2007, and gaining momentum during 2008–2009, the change program professionalised the intelligence role and introduced a “New Zealandised” version of the UK’s National Intelligence Model (2011, pp. 119–120). The program also repositioned New Zealand Police within the wider national security arrangements—with particular emphasis on transnational “wicked” issues such as illicit drugs and organised crime—through improved and closer relationships with other government agencies (2011, pp. 119–120). The changes within New Zealand’s largest security agency’s intelligence apparatus, and the potential longer-term impact of those changes on New Zealand’s whole-of-government approach to national security, evidenced by commentary in the Murdoch report (Murdoch, 2009, pp. 7 & 16), reinforced the need for coordinated and cooperative inter-organisational relationships between intelligence and law enforcement agencies.

The inter-organisational relationships brought about by the organised crime strategy and the changes to intelligence in New Zealand Police were patent examples of the coordination (refer to Figures 4.1 and 4.2), networked structures (refer to Figures 4.3 and 4.4), and both strategic and specific extents of engagement (refer to Figures 4.5 and 4.6) the government sought within New Zealand’s arrangements. The OFCANZ further enhanced those attributes by contributing the dimension of collaborative activity (refer to Figures 4.1 and 4.2) and strengthening the specific extent of engagement through its multi-agency taskforce approach to investigations (refer to Figures 4.5 and 4.6) (King, 2008; Organised and Financial Crime Agency New Zealand, n.d. (a)).

In undertaking its work, the new crime agency—described as a discrete service agency hosted by police (New Zealand Police, 2008, p. 16)—was expected by the minister of police to “work collaboratively with national and international law enforcement and intelligence agencies as well as border agencies …” (King, 2008a, p. 1). That pronouncement unambiguously presented the government’s collaborative expectation of the new agency. The statement also provided a concise summary of the approach New Zealand’s Government wanted to take to the “wicked” issue of organised crime and, due to the “pulse of globalisation” (Albanese, 2012, p. 3; Wood, 2006, p. 248), its close criminal companion transnational criminality. The minister’s collaborative expectation appeared to have been delivered with the agency’s website listing its “partners” as including, amongst others: “… Immigration New Zealand … New Zealand Police, New Zealand Customs Service … Department of the Prime Minister and Cabinet … Government Communications Security Bureau … [and] New
Zealand Security Intelligence Service …” (Organised and Financial Crime Agency New Zealand, n.d. (b)). Supporting the veracity of the website’s content was the fact that when a newly appointed minister of police was being briefed about the organisation, the work of the agency and its partners was described as “… run[ing] long-term multi-agency task forces against organised crime targets with assistance of partner agencies from across New Zealand and overseas” (New Zealand Police, 2011, pp. 36–37).

The final example to be referred to of New Zealand translating the desire for coordinated and collaborative activity into practice was the establishment of the National Cyber Policy Office. This was another new development that occurred during the 2011–2012 period (Ash, 2013, p. 5). The implementation of the office, within the prime minister’s department, recognised the transnational and cross-agency nature of the threats and risks emanating from the cyber world. The new office was tasked with focusing on coordinating the national cyber policy approach and enhancing collaborative cyber risk management endeavours across not only government agencies, but also the private sector and the community (Ash, 2013, pp. 2–6). That wide catchment of stakeholders—spanning government, business and individuals—arguably exemplified the impact that threats from transnational “wicked” issues were having on the relationships needed in New Zealand, and how they were being responded to by the government and its operational agencies.

Limitations
Every effort was made during the case study to locate and gather a comprehensive set of source documents to address the research question. However, in gathering the sources, some websites may have been missed, while alternative keyword/term searches may have produced different results.

DENMARK

Government Relationship Expectations
The Danish case study involved two data sets. Data set DK1 contained data related to inter-organisational relationships obtained from all the Danish sources gathered for the study. While data set DK2 was a sub-set of DK1 and contained inter-organisational relationship data about intelligence and law enforcement community engagement linked to transnational criminality. As a result of DK2 containing just nineteen items of data from five government sources about inter-organisational relationships, it was decided to use DK1 to analyse the government’s overall expectations when it came to relationships. That data set contained 76 items of data relating to government expectations, originating from nineteen government sources. It was felt, therefore, that DK1 data offered a broader view of the types of relationships and associated bureaucratic arrangements desired and supported by the Danish Government.

The government expectation data concerning relationship types (Figure 4.15) identified cooperation as the most often identified form of relationship, comprising 57 per cent of the data (n=43). Cooperation was followed by coordination with 22 per cent of identifications (n=17), while collaboration came next with seventeen per cent (n=13). The remainder of the government expectations related to networking (3 per cent) and autonomy (1 per cent). Mergers were not mentioned in the government expectation data. The inference
arising from these results was that the Danish Government was a strong supporter of cooperative relationships, while also being comfortable with coordination and collaboration being used.

In respect of structure, analysis of government data revealed the most commonly identified structures were networks (59 per cent, n=10) (Figure 4.16), while dyadic arrangements accounted for only a third of identified structures. That led to the inference that the Danish Government had a preference for the use of networked arrangements between its agencies, but still accepted dyadic relationships where they were appropriate.

Moving on to the extent of engagement within the relationships, government expectations data indicated that both strategic and specific engagement were sought with a 50/50 percentage split within the data (n=24) (Figure 4.17). That result indicated the government was comfortable with agencies working at both the strategic (i.e. development of policy and focus on joint goals/outcomes) and specific (i.e. addressing particular operational tasks and issues) levels of engagement in the relationships they formed.

**Figure 4.15. Danish Government relationship expectations (n=76)**

![Figure 4.15. Danish Government relationship expectations (n=76)](image)

**Figure 4.16. Danish Government relationship structure expectations (n=17)**

![Figure 4.16. Danish Government relationship structure expectations (n=17)](image)

On the qualitative front, the Danish Government’s inter-organisational expectations and responses to “wicked” issues were identified as linked to Denmark’s concept of security.
Larsen (2008, p. 91) described the security concept as broad in nature, encompassing both “hard” military issues and “soft” non-military issues (Archer, 2008, p. 7), such as those encountered in the contemporary security environment. That conceptual position was reinforced in the years following the end of the Cold War when the Nordic countries—including Denmark—refocused national security policies away from the over-arching threat of military conflict with the Soviet Union (Ulrich & Kivimaki, 2002, p. 25). During the period of refocusing, the Danes identified the country’s soft security concerns, in conjunction with their European Union (EU) partners, as a variety of transnational issues, including: environmental problems, border disputes, refugees, and organised criminality (Archer, 2008, p. 7 citing Petersen, 1996). Those concerns, originally articulated in the late 1990s, continued to be the focus of attention into the twenty-first century. That focus continued to be maintained into the years relevant to this study, but with additional dimensions stemming from the newly independent Baltic states (and other post-communist countries) following the collapse of the Soviet Union (Danish National Police, 2005, pp. 9–10; Ulrich & Kivimaki, 2002, p. 21).

In more recent times, the European Police Agency’s (Europol) 2011 organised crime threat assessment identified illicit drug flows, the trafficking of people, and the involvement of violent criminal organisations in cross-border smuggling as criminal activities impacting the Nordic countries (including Denmark) (Brady, 2007, p. 6; Europol, 2011, pp. 8–29). The Europol assessment also identified that the criminals responsible for those transnational crimes were also engaging in their own inter-organisational relationships with collaboration and cooperation between criminal groups being more evident in detected criminal enterprises (Europol, 2011, p. 5).

**Figure 4.17. Danish Government extent of engagement expectations (n=24)**

In analysing the inter-organisational relationship expectations and responses that the Danish Government supported with regards to the criminal threats outlined, the data identified the preference for a cooperative style of engagement (refer to Figure 4.15). That revelation supported Dalgaard-Nielsen’s (2006, p. 20) proposition that cross-agency cooperation was inherent in the bureaucratic culture of Denmark. The cooperative style also sat comfortably with two quite diverse, but arguably intertwined, scholarly views of Denmark. Those views highlighted that Denmark was a “small unitary state … [where m]any key persons … know each other personally and communicate regularly” (Dalgaard-Nielsen, 2006, p. 11), while, as a member of the Scandinavian group of countries (i.e. Denmark, Norway, and Sweden), it
enjoyed one of the “oldest and most entrenched democratic political systems” in the world (Weller, 2000, p. 172).

At the highest-level of government, persuasive data on the cooperative style was found in speeches given by the three Danish prime ministers (i.e. Ander Fogh Rasmussen 2007–2009, Lars Lokke Rasmussen 2009–2011, and Helle Thorning-Schmidt 2011–2012), who all held office during the study’s timeframe of 2007–2012. Each prime minister reinforced to the Folketing (Parliament) and to the nation—during their traditional New Year’s day speeches—that cooperation within the country, with regional partners (including the EU and the North Atlantic Treaty Organization (NATO)) and with others (such as the United States of America) was the way Denmark would ensure its security and best tackle issues such as transnational crime, illegal migration, and human trafficking (Rasmussen, A.F., 2008; Rasmussen, L.L., 2009; Thorning-Schmidt, 2011). That consistent reinforcement was not surprising given Denmark’s history and in particular the years since the end of World War Two. Cooperative approaches to issues were clearly in evidence during those years, via, for example: Denmark’s engagement with other Nordic countries through the Nordic Council, police co-operation, its engagement with the Council of Baltic Sea States, its membership of the EU since 1973, and the country’s 65 year-long role in NATO (Block, 2007, p. 381; Brady, 2007, pp. 12–13; Karlsson, 2012, p. 5; North Atlantic Treaty Organization, n.d., Member countries; Ulrich & Kivimaki, 2002, p. 25).

To implement the desired cooperative style, the data revealed that the Danish Government and its agencies used inter-departmental working groups as a means of cooperating and coordinating when it came to “wicked” issues. The inter-departmental working groups on human trafficking, counter-terrorism and deportation of terrorist suspects (Government of Denmark, 2011, p. 29; Ministry of Integration, 2008; Ministry of Justice, 2006) illustrated that concept. The working group to consider “administrative expulsion of foreigners who [we]re deemed a danger to national security” (Ministry of Integration, 2008) also demonstrated an intelligence and law enforcement community inter-organisational relationship at work, with both the Danish National Police and the “National Security Service” (an alternative English title for the Danish Security and Intelligence Service (PET)) being represented along with six other organisations—two of which were non-governmental associations (2008). The working group concept, like its coordination cousin the steering committee (discussed later), was used to deliver the government’s expected cooperative style within a networked structure designed to focus on particular strategic policy issues (refer to Figures 4.15 to 4.17).

Another strategic approach used by the Danish Government to enable its cooperative approach was what has been termed—for the purposes of this work—“responsibility shifting.” That approach saw responsibility for a particular function or functions being moved from one agency to another, while leaving the two impacted organisations otherwise intact and with their original identity, unlike the result of a merger. As far as inter-organisational relationships go, responsibility shifting shared none of the features of the four NC3 relationship types discussed earlier, however, after reflecting on the data it appeared the process was undertaken for reasons similar to those used to justify inter-organisational coordination (refer Tables 3.4, 3.5 and 3.6). The most relevant and illustrative example of responsibility shifting (and its coordinative justification) involved the Danish National Police and PET (see page 96 for
greater detail), while a separate and earlier example from 2004 was also encountered involving the Danish Emergency Management Agency’s ministerial reporting and departmental orientation re-alignment (Dalgaard-Nielsen, 2006, p. 12). More will be said about the concept later.

While responsibility shifting was one means identified for delivering coordination, and through it cooperation, a more common means revealed by the data was multi-agency action plans and their associated steering groups/committees (Government of Denmark, 2009, 2011; Danish National Police, n.d. (b), p. 9; Danish Security and Intelligence Service, 2010, p. 40; Den Boer, 2001, p. 267; Karlsson, 2012, p. 39; Rasmussen, A.F., 2008; State Prosecutor for Serious Economic Crime, 2010, p. 11). Multi-agency action plans and steering groups fit well with the inferences developed during the first tranche of government expectation analysis (refer to Figures 4.15 and 4.16) which confirmed cooperation, coordination, and collaboration, occurring within networked structures.

The plans and mechanisms discussed above, it was contended, also fit with the analysis results and inferences concerning the government’s extent of engagement data (Figure 4.17). Action plans, for example, were often created by multi-agency working groups and presented a strategic overview of a policy initiative including joint-agency goals and outcomes. They then went on to detail the operational delivery process linked to those goals and outcomes. Within the data three relevant examples of multi-agency action plans were identified. Those plans, with transnational criminal links, sought to address: human trafficking, prevention of extremism in young people, and the fight against terrorism (Government of Denmark, 2009, 2011; Danish Security and Intelligence Service, 2010, p. 40).

The Action Plan to Combat Human Trafficking (Government of Denmark, 2011) was particularly illustrative of the approach. The plan was published under the logos of four government ministers or agencies (i.e. Minister for Equality, Ministry of Justice, Ministry for Refugees Immigration and Integration, and Ministry of Foreign Affairs), and the content of the plan required cooperation and collaboration amongst the agencies involved (Government of Denmark, 2011). The breadth of the action plan’s inter-organisational relationship linkages could be gauged from the listing of sixteen government agencies, including the Danish National Police, as parties to its implementation (Government of Denmark, 2011, pp. 25–26). An example of the blurring of the internal and external as discussed by Bigo (2000, pp. 174–175).

The list of agencies party to the combating of human trafficking did not, unfortunately for this study, include direct reference to an intelligence service—thus establishing an explicit inter-organisational relationship link between the intelligence and law enforcement communities. However, the facts that PET: was an integral part of the Danish National Police (Weller, 2000, p. 172), included in its structure a Centre for Organised Crime (Danish Security and Intelligence Service, 2010, p. 68), and played a distinct role in Denmark’s immigration processes (2010, pp. 26–27) made it highly likely that the action plan implicitly included a cooperative and/or collaborative relationship with its security service.

Having canvassed the expectations, and mechanisms, of the Danish Government concerning inter-organisational relationships the analysis moved to explore the relationships being delivered by intelligence and law enforcement agencies.
**Intelligence Community Relationships**

In determining what types of relationship the intelligence and law enforcement communities delivered in Denmark (refer to Table 3.9), the intelligence community (IC) data were analysed first. For that analysis data set DK2 (n=54) was used. The data revealed that cooperation was the most often identified inter-organisational relationship (Figure 4.18) contributing 49 per cent of the data (n=28). Collaboration followed with 30 per cent of identifications (n=17), while coordination came third with 21 per cent (n=12). There was no data from IC sources for autonomy, networking or merger situations. Those results led to the inference that the IC was delivering relationships in general alignment with the government’s expectations.

Analysis of the data concerning the structures supporting relationships entered into by the IC identified an almost even split between networked (n=4) and dyadic (n=5) arrangements (Figure 4.19). The result led to the inference that both forms of structure were considered appropriate by the intelligence services. That state of affairs was not out of keeping with government expectations, however, it was noted the data sample for that analysis was small in size, consisting of only nine relationship identifications.

On the issue of extent of engagement (Figure 4.20), the data revealed 83 per cent of engagements were identified as involving specific matters (n=5), with seventeen per cent involving the strategic alternative (n=1). Again, it was noted that the data sample was small in size, consisting of only six identifications.

The final dimension of inter-organisational relationships to be considered was motivation. Analysis of motivation sought to assess the reasons why inter-organisational relationships were entered into. As outlined earlier, the reasons supporting formation of a relationship included legislation, encouragement, or a voluntary decision on the part of the organisations involved.

The DK2 data (Figure 4.21) revealed an almost even distribution across the three options with: 30 per cent of identified motivation being from legislation (n=3), 40 per cent from encouragement (n=5), while 30 per cent were identified as pertaining to relationships resulting from voluntary engagement (n=3). Those results led to the inference that the full range of motivational approaches was being used in Denmark when it came to intelligence agency relationships.

Moving to the second tranche of analysis involving the qualitative content of the data, a particularly useful example of IC inter-organisational relationships was found in sources originating from the Money Laundering Secretariat. The secretariat, housed in the office of the State Prosecutor for Serious Economic Crime (Money Laundering Secretariat, 2007, p. 4), was tasked with “collecting, registering, transferring, coordinating and processing information regarding the laundering of proceeds of crime and financing of terrorism” (2007, p. 4). In undertaking those tasks the secretariat engaged in “collaboration” with the security service to handle information concerning the financing of terrorism (2007, p. 4). That arrangement, involving as it did both coordination and collaboration between the Danish security service and law enforcement (2007, p. 8), was one of the earliest and longest-standing examples identified. Beyond information management, the secretariat also engaged with the security service via “a project group” comprising representatives of both organisations that “conduct[ed] investigations based on guide lines [sic] determined by the [MLS] steering
“The steering group” (2007, p. 8). The Money Laundering Secretariat/security service arrangements were, therefore, also illustrative of the steering group process used by the Danes to deliver coordination and cooperation.

Figure 4.18. Danish Intelligence Community (IC) relationships (n=54)

Figure 4.19. Danish IC relationship structures (n=8)
In a different area of Denmark’s security architecture, the Danish Emergency Management Agency’s (DEMA) arrangements and relationships also provided data relevant to the study. DEMA was tasked with responding to a range of emergencies including, for example, a terrorist attack in Denmark with transnational links. DEMA’s response to a national level crisis can include activation of what is known as the National Operative Staff (Dalgaard-Nielsen, 2006, p. 15; Danish Emergency Management Agency, 2012). The National Operative Staff was designed as a coordination group, working under the leadership of the national police, to “facilitate decision-making nation-wide across different sectors” (Danish Emergency Management Agency, 2012). The core membership of the operative staff was identified as the Danish National Police, Defence Command Denmark, and DEMA, with “relevant authorities” called upon to join dependant upon the crisis being faced (2012). That arrangement would, therefore, enable the security service and the foreign intelligence service to be engaged if, for example, the event were a terrorist attack with transnational links.

A further relationship connection between DEMA (and its operative staff partners) and the security service was the publicly acknowledged role PET’s assessments played in helping determine the national emergency management level for Denmark (Danish Emergency Management Agency, 2012). Thus, the National Operative Staff coordinating
arrangements and PET’s assessment link were viewed as evidence of the cooperation and coordination revealed in Figures 4.18 and 4.22, and in the inferences arrived at from them. Further adding to those findings was the fact that DEMA’s relationships also reflected the collaboration evident in Danish security arrangements through its contribution of staff to the Center for Terror Analysis (CTA) hosted by the security service (Danish Security and Intelligence Service, n.d. (a), Center for Terror Analysis).

The CTA was established in 2007 as an output of the Danish Government’s Action Plan for the Fight Against Terrorism (Danish Security and Intelligence Service, n.d. (a), Center for Terror Analysis). The center, like a number of its international counterparts, was designed as a multi-agency collaborative enterprise (Persson, 2013, pp. 15–16). As well as DEMA, the analysis centre was staffed by the security service, the Ministry of Foreign Affairs, and the Danish Defence Intelligence Agency (FE) (Persson, 2013, pp. 23–24). The center’s organisational arrangements and staffing exemplified the collaborative, networked, and specifically focused nature of Denmark’s transnational criminality response (refer to Figures 4.18, 4.19, 4.20, 4.22, 4.23 and 4.24). It was further contended that, through its CTA involvement, the security service—with its distinctive dual law enforcement/intelligence service character—made the center an example of Danish intelligence and law enforcement engagement. Another arrangement, potentially similar to the terror analysis center, appearing in the data involved the Danish Center for Cyber Security (CFCS) housed in the foreign intelligence service.

The cyber security center was a relatively new addition to Denmark’s defences against transnational threats, only coming into existence in 2012 (Danish Defence Intelligence Service, 2013, Foreword). While the foreign intelligence service was mandated as Denmark’s national information technology security authority (2013, pp. 20–21), the threats emanating from and occurring within the cyber domain spanned a number of Danish agencies remits. For example, scholars assessed cyber threats as including: online fraud, child exploitation, intellectual property piracy, distributed denial of service attacks, and cyber-warfare (Cox, 2012, p. 6; Smith & Grabosky, 2012, pp. 247–264). That variety of threats was acknowledged by the Danes through the list of organisations the new cyber security center reported it was engaged with (Center for Cyber Security, 2012); however, what was notable about the list was that there was no direct mention of law enforcement, unless law enforcement was grouped under the list’s apparent catch-all reference to “Government authorities, including military authorities and institutions” (Center for Cyber Security, 2012).

The lack of a direct reference to law enforcement was explored further by reviewing all sources containing references to the new cyber security centre. Those sources ranged from website pages published by the Danish Defence Intelligence Agency, to CFCS reports, through to press releases regarding the center’s establishment. The result of the review was that none of the sources revealed evidence that the Danes had engaged law enforcement in the center’s operations. That finding was despite the establishment of the cyber security centre being an opportunity to publicly reinforce collaboration between the intelligence and law enforcement communities in combatting cyber threats as scholars Smith and Grabosky suggested (2012, p. 246). The apparent missed opportunity, while acknowledged as a singular instance, may have been indicative of the continuing challenges within the Danish bureaucracy, and elsewhere (for example, regarding EU counter-terrorism arrangements, see
Fagersten, 2010) concerning development and delivery of inter-organisational relationships between the intelligence and law enforcement communities.

The challenge of creating and maintaining effective inter-agency engagements in the Danish environment was highlighted elsewhere in the data. Whilst occurring outside the study’s time period, it was observed that in the 2006 benchmarking of the security service (PET) and the Danish Defence Intelligence Agency (FE) by external reviewers, the need to build better relationships between the two intelligence services was reported (Tebbit, 2006, p. iii; Anonymous British Security Service Officer, 2006, p. 4). Both documents contained recommendations outlining additional steps that could be taken to bring the two services, and other elements of the Danish security system, closer together, particularly concerning counter-terrorism (Tebbit, 2006, p. iii; Anonymous British Security Service Officer, 2006, p. 5).

In respect of counter-terrorism, the FE benchmarking report identified a desire by law enforcement—communicated to the reviewer by PET—for “greater effort” concerning the attention paid to the law enforcement side of the problem by the foreign intelligence service (Tebbit, 2006, p. iii). Furthermore, the foreign intelligence benchmarking recommended instigating “joint [FE]/PET teams on particular topics,” (Tebbit, 2006, p. iii) indicating that joint working was not a feature of the two service’s interactions at the time of the review. Additionally, and apparently more importantly—in the reviewer’s opinion—there was an identified need for a mechanism, at government level, to provide:

… more regular guidance throughout the year for the combined [FE]/PET intelligence effort and, in particular, to *ensure that the work of the intelligence and policy communities are linked more closely* and brought to bear on the range of security problems facing the Danish Government and people. (Italics added) (Tebbit, 2006, p. iii)

Meanwhile, with regards to the security service, the benchmarking identified the “understanding between PET and other parts of the police of the handling of intelligence aspects of cases that may come to trial is not as strong as it should be” (Anonymous British Security Service Officer, 2006, p. 3). The point highlighted, that despite being “an integral part of the Danish Police” (2006, p. 2), there was still disconnection in the cooperation, coordination—and possibly even collaboration—occurring between the two parts of the one organisation.

The recommendations highlighted above suggested the need for increased coordination across the Danish intelligence community. Including, it was posited, in the definition of “security problems” (Tebbit, 2006, p. iii)—such as the “wicked” issues being addressed by the services that involved transnational criminality. Subsequent to the benchmarking being finalised, reporting by the Parliamentary Committee on the Intelligence Services indicated the recommendations from both reviews had been accepted by the Danish Government and implemented (Committee on the Intelligence Services, 2010, pp. 2–3). In particular, the recommendation for greater coordination of the intelligence services’ focus regarding the security agenda was reported as implemented, with a sub-group of the parliamentary committee on the security services being created to provide the desired guidance (Committee on the Intelligence Services, 2010, p. 11).

Finally, before concluding the IC analysis, a phenomenon occurring within the Danish national security bureaucracy involving the security service was considered worthy of
specific discussion. As previously stated, PET was deemed an integral part of the Danish National Police. However, as a result of changes arising from the 2006 benchmarking of the security service and from the Danish National Police embarking on substantive reorganisation from 2007 onwards (Holmberg, 2013, pp. 34), the data revealed the security service had commenced moving towards a more independent and ‘security service’ focused organisational identity and standing. The de-coupling could be viewed as a process of separating and administratively corraling the “high policing” activities (Brodeur, 2007, p. 27) undertaken by PET from the more routine, every-day “low policing” activities of the Danish police. That shift occurred over time and via a number of events, which are outlined chronologically below.

The first hint of the need for change came in 2006 when the security service benchmark reviewer stated there was a need for the distancing of PET from policing activities, and provision of “freedom to develop capabilities … necessary for its national security work” (Anonymous British Security Service Officer, 2006, p. 4). Subsequently, in 2010, two notable things happened. Firstly, a government committee reported that there was good reason to consider separating the security service’s annual budget from that of the Danish National Police (Committee for budget analysis of police, 2010, p. 63), while the second involved the security service publishing its first public biennial report on the organisation’s operational activities (Danish Security and Intelligence Service, 2010). The report—to be followed later by a similar one from the foreign intelligence service (Danish Defence Intelligence Service, 2013)—helped differentiate the agency and its work from that of the mainstream police.

Elsewhere in the source documents, it was observed that in material about biker and gang crime originating from the police between 2007 and 2010, the security service was not referred to as a participant (Danish National Police, 2008, 2009, 2010, 2011). However, in 2011 and 2012—in reporting from police on the same topic—PET was specifically identified, and separately to the Danish National Police, as one of the organisations involved in the multi-agency efforts to curb gang crime (Danish National Police, n.d. (a), n.d. (b)).

At around the same time, in 2011, the security service was, for the first time since its establishment, given a separate budget from that of the national police (Danish Security and Intelligence Service, n.d. (c), PET’s finances).

Then, in 2014, came a final substantive change that buttressed PET’s shift out from the shadow of its parent and onto its more independent standing. The change entailed the enactment of a new law regulating the security service’s work (Ministry of Justice, 2014). The law, which had been under discussion and development for some years, and which mirrored a similar new enactment regarding the activities of the foreign intelligence service, came into effect on 1 January 2014. Previously, PET’s legal foundation was found in the Policing Act (Danish Security and Intelligence Service, 2007, p. 15), which covered all of the activities of the Danish Police. The security service’s multi-year evolution into a more independent and accountable entity, while still remaining a part of its parent organisation, appeared complete.

While the change and its outcome were not examples of instituting any of the previously discussed inter-organisational relationship types, they were considered illustrative of Karlsson’s (2012, p. 5) description of the stable and slow pace of change encountered in the “historical institutions” of countries such as Denmark. That stable and slow change
process was, therefore, contended to be indicative of the measured and pragmatic approach to institutional change and relationships undertaken by the Danes and reported on by Gregory and Christensen (2004, pp. 75–76).

**Law Enforcement Community Relationships**

The analysis then shifted to the law enforcement community (LEC) and its inter-organisational relationship types \((n=11)\) (Figure 4.22). For that community, the data revealed coordination was the most often identified relationship type accounting for 40 per cent of relationships \((n=20)\). That was followed by collaboration with 34 per cent \((n=17)\) and cooperation with 26 per cent \((n=13)\). There was no data from LEC sources concerning autonomy, networking or merger, which was consistent with the previous intelligence community analysis. The inference drawn from the result was that the LEC was almost mirroring the result of their intelligence counterparts, and were behaving, therefore, in accordance with government expectations.

When it came to structures, the law enforcement data (Figure 4.23) revealed 62 per cent of identified structures were networked arrangements \((n=8)\), while 38 per cent concerned dyadic links. The resulting inference being, again, that the community was behaving as the government desired it too.

The extent of engagement was the next dimension analysed, and here the data showed that 69 per cent of identified extent of engagement involved specific issues \((n=11)\), while 31 per cent \((n=5)\) involved strategic matters. Again, the result was considered in alignment with the government’s expectations as outlined earlier.

The last relationship dimension to be analysed concerned what motivated the relationships (Figure 4.25). Here a different picture emerged to that revealed for the IC: 55 per cent of identifiable motivations were for legislative reasons \((n=11)\), 30 per cent were identified as voluntary \((n=6)\), and 15 per cent were identified as encouraged \((n=3)\). That resulted in an inference being formed, perhaps unsurprisingly for law enforcement agencies, that legislative permission was important in forming relationships. However, the outcome also revealed that agencies within the LEC were also prepared to exercise organisational prerogative to engage in relationships with others. It was contended that the detected willingness to exercise their organisational prerogative was founded on the strong influence that legislative and government support provided for such engagement (refer to Figure 4.25).
Having completed the first tranche of analysis, attention moved to the qualitative perspective. Here, the Danish National Police’s strategic plan to combat bikers\(^\text{19}\) and gangs (Danish National Police, 2011) was particularly illustrative of the relationships linking law enforcement and intelligence agencies in Denmark. The strategy, confirmed as a variant of an action plan, was a “classified working paper” (2011, p. 6) and was not, therefore, publicly available in its entirety as a source. However, reports on the progress being made delivering the strategy were published as unclassified documents and provided useful insight. Of particular relevance was that the data confirmed the strategy used a multi-agency steering group to coordinate a multi-agency element of its operational activity known as Task Force East (State Prosecutor for Serious Economic Crime, 2011, p. 11).

\(^{19}\) In Denmark, “bikers” was a term used to describe groups that in other jurisdictions were referred to as outlaw motorcycle gangs. The outlaw motorcycle gang label most commonly included well-known groups such as the Hells Angels, Bandidos and Comancheros. The Hells Angels and Bandidos were groups identified by police as having a presence in Denmark (Danish National Police, 2009, pp. 30–36).
Task Force East’s steering group brought together staff from the Danish National Police, various state prosecutors’ offices (including the State Prosecutor for Serious Economic Crime), tax authorities, five police districts within Zealand and PET (Danish National Police, n.d. (b), p. 9; State Prosecutor for Serious Economic Crime, 2011, p. 11). One output from the steering committee’s coordination role was multi-agency investigative collaboration between members of the task force, including the Zealand police, national police, and tax authorities (Danish National Police, n.d. (b), p. 9). The strategy’s use of a steering group and Task Force East’s subsequent inter-organisational investigative activity fits all the revelations arising from the quantitative analysis of intelligence and law enforcement relationships, namely: cooperative, coordinated, and collaborative engagement, involving networked structures, focused on specific operational issues, and motivated by a permissive legislative environment and government encouragement (refer to Figures 4.18, 4.19, 4.20, 4.22, 4.23 and 4.24). The task force arrangements outlined above fit with Brady’s (2007, p. 13) description of how Denmark sought to “avoid duplication and inhibiting efforts by ensuring that their police, customs and tax officials work together in single teams when dealing with organised crime.”
The security service’s engagement in the activities of Task Force East was illustrative of the previously mentioned Danish approach entitled responsibility shifting. For example, in 2006 the justice minister announced, as part of the Government’s Action Plan on Combating Terrorism—and in line with the recommendations from an inter-departmental working group—that elements of the police’s National Investigation Center (NEC) would move to become part of PET (Ministry of Justice, 2006). The minister described the move as helping to “strengthen the operational activity of the terrorist area” (2006). A key component of the shift was the security service also assuming responsibility for “the most serious organised crime” as well as domestic counter-terrorism (2006).

It was contended that the NEC-to-PET responsibility shift could best be characterised as coordinative with the government’s desire for that being quite explicit in the minister’s announcement of the change (Ministry of Justice, 2006). For instance, under the new arrangements the security service would initially develop intelligence-led serious organised crime or terrorism cases and then pass them on to the police for evidence-focused investigation (2006). The NEC-to-PET responsibility shift, however, also raised concern regarding its potential to have a negative effect on coordination. That concern was expressed during the government initiated benchmarking of the security service by a senior officer from the British Security Service (Anonymous British Security Service Officer, 2006). In the reviewer’s report, he/she pointed out that the NEC-to-PET move may in fact “blur roles and accountabilities between PET and the police” (Anonymous British Security Service Officer, 2006, p. 3). However, no data regarding the concern materialising was found in the sources gathered for the case study.

Beyond the specific response to organised crime detailed above, the Danish LEC, and in particular the police, also received a range of other supporting services from PET. The security service’s website (Danish Security and Intelligence Service, n.d. (b), n.d., About PET), for example, listed seven notable functions provided by the security service to assist the police, which included: the Special Intervention Unit (providing assistance with high risk activities such as hostage and dangerous arrest situations), the Surveillance Unit (assistance with difficult and cross-border monitoring tasks), the Technical Support Unit (assistance with tasks such as video-surveillance, tracking and interceptions), and the Special Operations unit which handled “sources” described as “informants and civilian agents … persons who in general provide PET with information” (n.d. (b), n.d.). The range and nature of those services constituted, it was posited, the essence of the inter-organisational relationships identified during the first tranche of analysis, and sought by the Danish Government via its expectations (refer to Figures 4.15, 4.18 and 4.22 above).

While data concerning links between the Danish foreign intelligence service (FE) and law enforcement were, to say the least, sparse, data regarding the operation of the Center for Terror Analysis (CTA) provided at least a glimpse of formal inter-organisational engagement taking place. As previously detailed, CTA included both security service and FE staff in its workforce. Furthermore, given the role analysis centre assessments played in informing the Danish security system about threats (both internal and cross-border), and the acknowledged blurring of the distinction between external and internal threats (Danish Defence Intelligence Service, n.d. (b), 28.02.2013; Danish Defence Intelligence Service, 2013, p. 18), it was apparent that there were very likely to be cooperative, and possibly even
collaborative, links between FE and law enforcement. That assessment was notwithstanding the earlier discussion of how the foreign intelligence service appeared to have left law enforcement out of the equation when it came to the establishment and publicising of its new cyber security centre.

Limitations

Every effort was made during the case study to locate and gather a comprehensive set of source documents to address the research question. However, in gathering the sources, language differences may have meant that some websites were missed, while alternative keyword/term searches may have produced different results. The fact that none of the sources gathered from the Danish Defence Intelligence Service (FE) provided data concerning inter-organisational relationships was a specific limitation associated with the intelligence community analysis aspect of the case study. A further limitation encountered in respect to the case study was that the Danes used one word to describe both cooperation and collaboration in Danish language sources, and the apparent indiscriminate use of those two English words when Danish sources were translated into English by their authors. As detailed in the methodology chapter, emphasis was placed on examining the context surrounding relationship related text to help distinguish between cooperation and collaboration. If a clear distinction could not be made, the relationship was not included in the data for the case study.

FINLAND

Of note regarding the Finnish case study, in comparison to the previous two, was that it was necessary to title the section regarding intelligence community relationships Intelligence Relationships as it only contained analysis of data regarding the Finnish Security Intelligence Service. As detailed earlier in the methodology section, Finland only has a domestic security service; therefore, the term intelligence community was not appropriate.

Government Relationship Expectations

Analysis of relationship data obtained from Finnish Government sources (Figure 4.26), confirmed cooperation as the most often identified relationship type, comprising 51 per cent of relationships (n=54). Cooperation was followed by coordination, which comprised 36 per cent (n=38), with collaboration next, comprising ten per cent (n=11). The remaining government expectation data confirmed networking comprised three per cent of identified relationships (n=3), while autonomy and merger were not mentioned in the data at all. Therefore, the inference developed regarding government expectations was that cooperative relationships predominated in the Finnish context. Furthermore, those cooperative relationships were supported by inter-agency coordination, and to a lesser degree collaborative activity. The remaining three relationship types (i.e. autonomy, networking, and merger) were not featured (or were only in a minor way) in the Finnish environment.

Examination of the government expectation sources from which the data were obtained, confirmed they consisted of documents detailing strategies, programs, action plans, and legislation; for example: the Security of Society Strategy, the Action Plan to Prevent Violent Extremism, the Internal Security Programme, the National Counter-terrorism
Strategy and the Police, Customs and Border Guard Cooperation Act\textsuperscript{20} (Security and Defence Committee, 2008; Ministry of the Interior, 2008a, 2010a, 2012).

**Figure 4.26. Finnish Government’s relationship expectations (n=106)**

![Diagram showing relationship expectations]

Analysis then moved to identifying the inter-organisational structures that the government expected to support their relationship preferences (Figure 4.27). The analysis revealed the most often identified structures were networks (93 per cent, \(n=27\)), while dyadic structures accounted for seven per cent of identifications (\(n=2\)). The inference drawn from the analysis was that the Finnish Government used multi-agency structures to underpin their cooperative, coordinated and collaborative arrangements, rather than a more fragmented dyadic agency-to-agency approach.

**Figure 4.27. Finnish Government’s relationship structure expectations (n=39)**

![Diagram showing relationship structure expectations]

The next dimension of inter-organisational relationships to be considered was the extent of engagement expected between the agencies (Figure 4.28). Analysis revealed that almost two-

---

\textsuperscript{20} The full English language title of the Act was: *Act on Cooperation between the Police, Customs and Border Guard (687/2009)* (FIN). In Finland it was commonly reduced to the acronym PTR, which in the Finnish language stood for: Poliisi, Tulli and Rajavartiolaitos (Police, Customs and Border Guard). In Finnish source documents published in English the PCB acronym was used. Throughout the case study the Finnish acronym PTR was used to refer to the cooperation arrangement.
thirds of identified extent of engagement (63 per cent, n=40) related to specific issues and tasks (n=24), while strategic engagement accounted for 37 per cent (n=24). The inference drawn from the analysis was that, while the government supported some operational agency activity at the strategic level concerning the response to be taken to “wicked” policy issues, the primary focus of government expectations was on agencies engaging in the delivery of activity aligned to specific issues and tasks.

**Figure 4.28. Finnish Government’s extent of engagement expectations (n=64)**

The extent of engagement results were deemed consistent with the Finnish approach of developing programs, strategies or action plans using multi-disciplinary working groups at both ministerial and official levels to detail the specific aspects of each agency’s contribution in responding to “wicked” problems (for example, see Ministry of the Interior, n.d., 2008a, p. 1). Agencies then focused on delivery, using steering groups to help coordinate their actions (for example, see Ministry of the Interior, 2008a, p. 74, 2008b, Summary: para 14).

Having completed the first tranche of analysis, focus shifted to the qualitative aspects of the data and what examples it could provide illustrating the inferences occurring in practice. Overall, it was clear from Finnish Government sources and data that cooperation amongst agencies was the essence of the way things were done in Finland. Evidence of that approach was found at the highest levels of the government with, for example, Prime Minister Vanhanen (Prime Minister’s Office, 2008), stating during discussions with a representative of the European Commission “… [that] close cooperation is needed to improve internal security and prevent organised crime in the region.” A month later the prime minister used the opportunity of a security policy seminar (Vanhanen, 2008) to reiterate his view with regards to Finland’s response to “new threats,” when he said:

New threats are best countered through co-operation with others and preparation. In order to achieve broad security, we must be ready to assume a role in crisis management and we must have seamless co-operation between various authorities. Within this new concept of broad security, the military takes a back seat … we have a carefully planned and implemented crisis management system, which is based on legislation and the co-operation of competent authorities.

While on that occasion the prime minister was discussing the broader approach being taken to security policy and crisis management, cooperation had been specifically enshrined in the
government’s policy on internal security (Ministry of the Interior, 2008a). The Internal Security Programme (ISP), to give the policy its formal title, was the result of wide-ranging coordinated and cooperative consultation “involving almost 200 experts from 12 ministries, 22 government offices and agencies and 23 NGOs” (2008a, p. 1)—a clear example of the inferences developed after consideration of Figures 4.26, 4.27 and 4.28 above. The ISP outlined the Finnish Government’s response to “wicked” problems spanning a spectrum of challenges that included: “… the fight against organised crime, containment of extremist movements, [and] anti-terrorist activities” through to “illegal migration and human trafficking” (2008a, p. 1). Again, a common list of threats can be seen emerging as discussed by Bigo (2000, p. 174) and identified in both the New Zealand and Danish case studies.

The 2008 ISP document was described as a “government resolution that specified the priorities, objectives and measures for the inter-sectoral development of internal security” (Ministry of the Interior, 2008a, p. 5). The program’s role was to enable Finland to attain the government’s strategic goal of being “the safest country in Europe in 2015” (2008a, p. 6). To achieve that goal the government identified that the country needed to overcome a number of key challenges. Three of those challenges were the transnational crime infused “wicked” problems of: “cross-border crime” (which included: drug and substance smuggling, procuring [women for prostitution], illegal migration, counterfeiting, and property crime); “cybercrime” (which included: online crimes, such as data break-ins, denial of service and identity theft; illegal information content, such as incitement, sexual abuse and copyright breaches; and ordinary crimes, such as fraud and forgery); and “terrorism and violent extremism” (which included: radicalisation, violence against the public, and threats targeting countries responding to extremist violence) (Ministry of the Interior, 2008a, pp. 13–15).

Within the ISP, the responses to the challenges were grouped under two broad headings. One dealt with general objectives and measures pertaining to the full-range of challenges, while the second—and more relevant to the study—spelt out “particular objectives and measures to improve internal security” (Ministry of the Interior, 2008a, pp. 27–72). In that section each challenge was broken down to identify which ministries and agencies would tackle each component (for example, see “National and international cooperation between authorities in combating organised crime will be enhanced,” 2008a, p. 65). For each challenge a “principal responsibility” was assigned to one ministry (i.e. Ministry of the Interior), and then the document listed the “also involved” ministries and agencies (2008a, pp. 27–72). Thus, the Finnish Government identified who the coordinating authority was, and who the cooperating participants in each case were—an approach indicative of the picture presented by Figures 4.26, 4.27 and 4.28 above, and the inferences drawn from them. That approach also aligned with Alter and Hage’s (1993, p. 93) description of “interorganizational coordination … towards] … common objectives and [a] supraorganizational goal”. Furthermore, the Finnish networked structural arrangements, spelt out in the security program, were illustrative of Whelan’s (2012, p. 51) description of how such coordinating activities arose and operated. In the ISP’s case it was through formal establishment of a network with an identified leader, who was invested with the power to coordinate the network’s activities.

The security program was one of a number of Finnish Government sources that reflected Whelan’s (2012) description, and that were viewed as indicative of the Finnish cooperative and coordinated approach being applied. Another source of particular relevance
to the research was the National Counter-terrorism Strategy (Ministry of the Interior, 2010a). The strategy identified:

In Finland, the police have the primary responsibility for combating terrorism. However, the capability to effectively fight terrorism requires continuous and consistent cooperation not only between all security authorities but also other authorities and a wide range of other actors … the underlying theme of this strategy … to further develop cooperation and coordination. (2010a, pp. 3–4)

However, perhaps the singular example illustrating the Finnish Government’s overall inter-organisational expectations being codified and operationalised was the enactment of the *Act on Cooperation between the Police, Customs and Border Guard* (687/2009) (FIN), referred to hereafter as ‘the cooperation Act’ or the *PTR Act* (2009). The cooperation Act replaced an earlier government issued cooperative decree, in place since 2001 (*PTR Act*, 2009, p. 5). The cooperation Act, while proclaiming, via its title, to focus on cooperation, was assessed to also require the three organisations it pertained to, to engage in coordination and collaboration. The cooperation Act, therefore, encapsulated all three inferences drawn from Figures 4.26, 4.27 and 4.28 above. For example, with regards to coordination, section 9 of the *PTR Act* (2009) stated:

> [PTR] authorities shall set the objectives for international cooperation, and agree on joint international measures and on the participation in operation on a national basis and in advance of any action so that consideration is given to the tasks and powers of each [PTR] authority. (*PTR Act*, 2009, p. 4)

Elsewhere, in section 7 of the *PTR Act* (2009, p. 4) the three organisations were empowered to “establish a joint criminal intelligence and investigation team for the purposes of preventing, detecting or investigating a crime or a series of connected crimes.” Such multi-disciplinary teams are emblematic of collaborative activity, given they involve the giving up of ‘organisational turf’ in order for people from alternative disciplines to work effectively together (Axelsson & Axelsson, 2006, p. 81; Farmakopoulou, 2002, p. 53).

A further Finnish inter-organisational relationship concept illustrated by the cooperation Act was that of a networked structure underpinning the relationship types, as depicted in Figure 4.27 (also see Figures 4.30 and 4.34 below). In the Act’s case it was a network involving the three primary law enforcement organisations, namely the police, customs and border guard. Furthermore, it was argued that, due to Finland’s security architecture having the security intelligence service as an integral part of the police (Holmström, 2013, p. 265), the *PTR Act* (2009) also linked the intelligence service to the cooperative arrangements—under the broader police banner. That contention was separately supported by data from two other source documents. The first was a working group report to the minister of the interior (Ministry of the Interior, 2008c, pp. 21–26) concerning recommendations on the future structure of police administration (2008c, cover letter), while the second was a Customs’ intelligence and investigation report regarding operational activities during 2008 (Finnish Customs, 2009b, p. 32). The content of those documents will be discussed later in regard to the relationships of the intelligence service in the next section.

The final government relationship dimension able to be garnered from review of the cooperation Act was the rationale behind the government’s inter-organisational relationship expectations. Section 1 of the *PTR Act* (2009, p. 1) stated that one of the purposes of the Act
was to see that “cooperation is carried out in an appropriate, efficient and cost-effective manner.” The references to efficiency and cost-effectiveness were echoed in other source documents regarding: the security of society, security research, and Finland’s 2012 security and defence policy (Security and Defence Committee, 2008, p. 3; Advisory Board for Sectoral Research, 2009, p. 10; Prime Minister’s Office, 2013, p. 93).

Elsewhere in the sources, cost-effectiveness was linked to a second concept of apparent importance to Finland, namely the avoidance of duplication (or overlap as it was sometimes referred to) in activities by government organisations. Avoidance of duplication was mentioned in a number of sources, including those dealing with Finland’s cyber security strategy, order policing, and the preparedness and comprehensive security program for Finland (Ministry of Defence, 2013, p. 11; Ministry of the Interior, 2007, p. 34; Preparedness and Comprehensive Security Committee, 2011, p. 86). The prevalence of mentions about cost-effectiveness and non-overlapping activities led to the view that they were both important factors in the rationale behind the Finnish Government’s expectations regarding inter-organisational relationships.

Intelligence Relationships

Moving on from the government’s expectations and looking at the delivery of relationships by operational agencies (refer to Table 3.12), the security service was analysed first. The analysis revealed that cooperation was the most often identified inter-organisational relationship type with 80 per cent of identifications (n=4) (Figure 4.29). Collaboration followed with twenty per cent (n=1). Given the small amount of data available for analysis in data set FD2 (n=5), FD1 was also reviewed to see if the thirteen items of security service data there indicated any difference to the above outcome. The result of that review was confirmation that cooperation remained the most prevalent relationship identified with 61 per cent of the data (n=8). It was followed by autonomy with 23 per cent (n=3), and then coordination and collaboration with eight per cent each (n=1 respectively). Networking and merger were not mentioned. Overall, the two analyses led to the inference that the security service was delivering predominantly cooperative relationships, with instances of autonomy, coordination and collaboration in evidence. That inference was in general alignment with the expectations of the Finnish Government discussed earlier.

In respect of the structures underpinning security service relationships (Figure 4.30), analysis revealed the only identified structures were networks (100 per cent, n=2). It was acknowledged that the data available for that analysis was very limited with only two structural identifications being made. However, the analysis led to the only possible inference that was, again, that the structures supporting security service relationships aligned with the government’s expectation. Further reflection on the sources of the data that contributed to the result determined that security service’s networks were linked to the PTR Act (2009) cooperative arrangements.

Figure 4.29. Finnish security service relationships (n=5)
Moving to the extent of engagement within the security service’s relationships (Figure 4.31),
the data revealed 100 per cent of engagements involved specific (i.e. issue or task focused)
matters (n=5). Again, alignment with the government’s expectations was confirmed; however,
absence of the security service’s involvement in strategic engagement (i.e. policy setting and
joint outcomes/goals development) was noteworthy. Closer examination of the sources and
data indicated the probability that the outcome was the result of the security service being an
integral part of the police. The suggestion being that strategic engagement, if it was happening,
was occurring at the national police organisational level, without making particular mention
of the security service arm of that larger entity (see Figure 4.35).
The next dimension of inter-organisational relationships to be considered was motivation. Analysis of motivation sought to assess what the principle reasons for inter-organisational relationships being entered into were. The Finnish security service data in FD2 (Figure 4.32) revealed 100 per cent of identified motivations related to legislation (n=5). That led to the inference that a permissive legislative mandate was pivotal to the forming of relationships by the security service.

Having developed a series of inferences from the Finnish security service data, consideration shifted to what the qualitative data was able to show regarding the service’s relationships. The intelligence service sources and data identified that the service carried the mandate in Finland for counter-terrorism cooperation as the “authority in charge of national and international cooperation among authorities” (Finnish Security Intelligence Service, n.d., p. 8). The security service identified one of the drivers for that cooperative mandate as the need for “maximal utilisation of resources allocated to counterterrorism by authorities and organisations” (n.d., p. 8), again raising the concepts of cost-effectiveness and avoidance of duplication that were evident in the Finnish Government data. Cooperation as a means of ensuring the efficient utilisation of resources was a concept supported in the scholarly literature by Himmelman (2002, p. 2) who confirmed resource sharing as a reason for cooperation; however, other scholars, such as Mattessich and Monsey (1992, p. 42), viewed resource sharing as more indicative of coordination or collaborative ventures.
As mentioned earlier, two particular publications reinforced the view that the security service worked in a cooperative fashion with other Finnish agencies. The first example was from a working group’s report on police administrative changes (Ministry of the Interior, 2008c). The report confirmed that the tasks of the Finnish Security Intelligence Service (Supo) included “counter-espionage, counter-terrorism, the state of internal security threats, preventive security and security guarding … The Security Police also participate in international organized crime fight [sic] …” (2008c, p. 21). Those tasks, and the potential for cross-border activity associated with most of them, made it probable that the security service worked cooperatively with the customs and border guard organisations in Finland under the provisions of the PTR Act (2009). The second example came from Finnish Customs reporting on its intelligence and investigation activities in 2008 (Finnish Customs, 2009b, p. 32). In that reporting, the security service was mentioned as one of two organisations “reinforcing” the establishment of a “temporary situation centre based on the [PTR] activity … [for the] … OSCE 2008 meeting of foreign ministers” (2009b, p. 32). Subsequent review of the PTR Act (2009), given its pivotal association with both examples, confirmed there was nothing in it that ring-fenced any police responsibility (for example, Supo’s tasks) from application of the Act’s provisions.

Elsewhere in the sources concerning the security service, data concerning a joint agency investigation further confirmed the supposition that inter-organisational relationships were taking place between customs, police, and the security service. The data in that particular case was related to another “wicked” transnational crime issue, namely weapons proliferation. In the first of two media releases (National Bureau of Investigation, 2011), the National Bureau of Investigation (NBI) confirmed that “the police and customs” were engaged in investigation of a suspicious cargo on a ship docked at a Finnish port. The linkage between the story and security service (who were not mentioned in the story) was that the release was located on the security service’s website (i.e. www.supo.fi), and the cargo under investigation was “69 Patriot missiles” (2011). Given the security service’s task of “… cooperat[ing] with other authorities on proliferation control” (Finnish Security Intelligence Service, n.d., p. 24), it is reasonable to surmise that the service was a party to the police element of the investigation, alongside its sister unit the NBI.

In the second press release on the same topic (National Bureau of Investigation, 2012), the “joint investigation team of the customs and police” were reported to have continued their work. The second media release was also located on the security service’s website, once again supporting the view that Supo was an active cooperative partner in the investigation. The concept of a joint investigation team was described and authorised in the PTR Act (PTR Act, 2009, p. 4), and—as previously argued—that Act also applied to the security service, as well as the other elements of the Finnish Police. The term ‘joint investigation team’—discussed earlier in connection with the PTR Act (2009) and assessed as describing collaborative activity—appeared elsewhere in the data, primarily concerning the delivery of LEC relationships and it will be discussed further in that part.

21 The National Bureau of Investigation (NBI) was one of three national police units in Finland. The other two were the Finnish Security Intelligence Service (Supo) and the Police College of Finland (Finnish Police, n.d., n.d.). The NBI’s role was described as: “specialises in combating organised and professional crime” (Ibid).
Law Enforcement Relationships

Having examined the delivery of relationships by the security service, attention shifted to the Finnish law enforcement community (LEC). The first tranche of analysis for that community revealed cooperation was again the most prominent relationship amongst those identified (Figure 4.33), accounting for 46 per cent of the data (n=27). Cooperation was followed by coordination with 32 per cent of identifications (n=19), and then came collaboration with 22 per cent (n=13). No data were recorded for the relationship types of autonomy, networking or merger. Those results mirrored the ones obtained for the government’s expectations and the security service’s delivery of relationships. The inference resulting from the above outcome was that the LEC was delivering relationships in accordance with government expectations. On closer examination, the LEC data were found to have originated from sources that described involvement in government strategies, programs and action plans. For example, two sources of particular relevance were the Internal Security Programme (Ministry of the Interior, 2008a) and the Action Plan against Illegal Immigration (Ministry of the Interior, 2012a). Finnish Customs also contributed to the outcome through its annual report and annual intelligence and investigation reports (Finnish Customs, 2009b, 2012, 2012a). Further discussion of those documents will occur later.

Figure 4.33. Finnish Law Enforcement Community (LEC) relationships (n=59)

Having canvassed inter-organisational relationship types, analysis moved to data regarding the structures underpinning the relationships and extent of engagement involved in them. In regards to structures (Figure 4.34), analysis revealed that most identified structures were networks (95 per cent, n=21), while dyadic arrangements accounted for five per cent (n=1). Once again, the LEC structural results led to the inference that the community delivered inter-organisational structures that aligned with the government’s expectations. The structural data were principally influenced by sources that referred to the PTR Act (2009) arrangements that had created a strong tripartite network between three of the four agencies in the LEC.

Moving to the extent of engagement within the relationships (Figure 4.35), 80 per cent of the LEC’s engagement were identified as involving specific issues (n=24), while twenty per cent (n=6) related to strategic matters. Those results appeared consistent with the government’s expectations and to the security service’s result. That outcome led, yet again, to the inference that the LEC were in alignment with the government’s expectations. The data involved originated from sources that discussed the involvement of enforcement agencies in
programs, strategies and action plans using multi-disciplinary working groups at both ministerial and official levels (for example, see Ministry of the Interior, n.d., 2008a, p. 1).

The final dimension of the LEC’s inter-organisational relationships to be considered was motivation. Analysis of the data (Figure 4.36) revealed 71 per cent of identified motivations related to encouragement (n=20), while 29 per cent were coded as legislated (n=8). Voluntary engagement had no data recorded for it. The inference formed from that result, and examination of the sources that had contributed, was that the strategies, programs and action plans which law enforcement were engaged with were structured and presented in a way that encouraged inter-agency engagement, while leaving the legislative requirements of the PTR Act (2009) sitting quietly in the background. That approach allowed the agencies concerned to continue to operate within the bounds of their organisational legislation while at the same time applying the principles of the cooperation Act to the strategies, programs and action plans they were involved with.

Division of organisational activity within the Finnish bureaucracy according to legislation and agency mandates appeared to be a central feature of the country’s arrangements. For example, section 10 of the Government Rules of Procedure (262 C.F.R. (2003) (FIN), p. 10) discussed the “competent ministry” and stated “[m]atters shall be divided up according to the ministries’ mandates as laid down in the Chapter,” while a media release in respect of the national counter-terrorism strategy stated “[t]he strategy contains five strategic guidelines and ensuing recommendations for action which fall under the mandate of various authorities” (Ministry of the Interior, 2010).

Beyond the formation of inferences based on the quantitative data, on the qualitative front, the four law enforcement organisations discussed in various source documents how they were engaging in inter-organisational relationships, particularly those premised around the joint-working concept. For example, Finnish Customs, in its 2011 annual report (Finnish Customs, 2012, p. 15), noted in respect of the action plan for dealing with illegal immigration:

Customs … have an important role in prevention of serious crime …[g]ood opportunities to carry out this role have been provided by the act on cooperation between the Police, Customs and the Border Guard and the joint [PTR] criminal intelligence units and joint information management projects, as well as by joint representation at international forums. (2012, p. 15)
Customs’ description of the role they performed in crime prevention was further borne out by the Finnish Police in their 2012 annual report (Finnish Police, 2013). In that reporting, police highlighted how they were taking “target-specific action” against “the most serious and organised crime” using joint-analysis and multi-agency projects focused on internationally mobile groups of criminals (2013, p. 8). Police directly linked the joint-working arrangements to the PTR cooperation model. Furthermore, police described how they had extended the arrangements beyond their two formal partners in the model, to include “the Finnish Prosecution Service and Europol” (2013, p. 8), an example of an institutional security network being linked to an “international security network” (Dupont, 2007, pp. 80–81).

On the frontier, the Finnish Border Guard (the third party to the PTR Act (2009)) also promoted their inter-agency activities and relationships through, for example, the content of their Border Guard Strategy 2022 (Finnish Border Guard, 2012). In highlighting their cross-border crime responsibilities in the strategy (2012, p. 28), the border guard also drew attention to the “close cooperation with other law enforcement authorities” which saw them working with police and customs (2012, p. 29). In fact the border guard valued cooperation so highly they included it as one of their three organisational values (the other two being reliability and competence), and mentioned it in their vision statement: “The Border Guard is a cooperative, internationally renowned expert in border management …” (2012, p. 28). That commitment to cooperation was not surprising given the minister of the interior’s statement, during an...
interview for the border guard’s in-house magazine (Kaasinen, 2011, p. 1), that “… inter-agency cooperation – this is something that can be taken even further” while also, again, linking the concept to efficiency and avoidance of duplication (2011, p. 1).

Figure 4.36. Finnish LEC relationship motivations (n=28)

Finally, from the law enforcement perspective, the Finnish Immigration Service (FIS) also promoted inter-organisational relationships as integral to their work. In 2009, via a press release about their 2008 annual report, the immigration service drew attention to the new immigration case management system (Finnish Immigration Service, 2009), which they described as “… a genuine inter-authority system, used in liaison between many authorities, including … the police, the Finnish Border Guard and Finnish missions abroad.” Three years later, the FIS stated, in its 2011 annual reporting, that the agencies new strategy confirmed the need for “… seamless cooperation with all our partners … Finnish Police and Finnish Border Guard” (Finnish Immigration Service, 2012). The immigration service continued that theme, later in 2012, but went slightly further by explaining that the “close cooperation with the police and Border Guard” was happening on a “daily basis” (Finnish Immigration Service, 2012a). While law enforcement cross-agency cooperation was evident from the above immigration service examples, and through the data charted in Figure 4.33, there was data that indicated the security service were also, in all probability, a party to that activity.

The most comprehensive example of that probability existing came from the Action Plan Against Illegal Immigration 2012–2015 (Ministry of the Interior, 2012a). The document confirmed that as well as the police, border guard and immigration service deploying “joint ILO [Immigration Liaison Officer]” positions in four off-shore locations (2012a, p. 12), the security service was reinforcing the work against illegal migration through “… short term officers posted at certain Finnish foreign missions to provide support to the missions as they investigate fulfilment of the requirements for entry” (2012a, p. 13; Teirilä, 2015, p.p. 221–222). On the same immigration theme, the Finnish Aliens Act (301/2004) (FIN) authorised the security service to undertake interviews regarding asylum investigations and to be one of four named police entities whose “… commanding officer … [could decide to] … hold an alien in detention …” (2004, pp. 35–43). Those linkages, it was contended, provided yet further support for the assessment that the Finnish security service did engage in a variety of inter-organisational relationships with the LEC as outlined earlier through the inferences developed in regards to Figures 4.49 to 4.32.
Limitations

Every effort was made during the case study to locate and gather a comprehensive set of source documents to address the research question. However, in gathering the sources, language differences may mean some websites were missed, while alternative keyword/term searches may have produced different results.
CHAPTER 5 CASE STUDY COMPARISON AND DISCUSSION

DISCUSSION

On completion of the three case studies the findings from them were combined into a set of comparison tables. A table was created for each of the categories used in the case studies, namely: government expectations, intelligence community (IC) relationships, and law enforcement community (LEC) relationships. The government expectations table contained three sections, one each for the case study findings pertaining to the RC dials (i.e. relationship types, structures, and extent of engagement—see Figure 2.1). The IC and LEC tables contained the same three sections, but included a fourth to record the identified motivations that spurred the identified relationships. The three tables and the discussion associated with them are presented below. The discussion and resulting conclusions were then considered from a global perspective in order to determine what policy and practice benchmarks and implications the aggregated case study findings revealed.

Government Expectations

The findings presented in Table 5.1 reflect, it was contended, that the governments in the case study countries had recognised the need to avoid siloed delivery of responses to “wicked” security issues. The governments each displayed an expectation for inter-organisational engagement between their intelligence and law enforcement communities, and actively pursued policies aimed at delivering those relationships. For reasons of history and culture the policies and activities differed slightly country-by-country in their shape and style, but they all ultimately sought to achieve a similar joined-up working outcome.

Table 5.1. Government relationship expectations comparison

<table>
<thead>
<tr>
<th>Relationship continuum</th>
<th>Denmark</th>
<th>Finland</th>
<th>New Zealand23</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Relationship types</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cooperation</td>
<td>Cooperation</td>
<td>Cooperation</td>
<td>Coordination</td>
</tr>
<tr>
<td>Coordination</td>
<td>Coordination</td>
<td>Collaboration</td>
<td>Collaboration</td>
</tr>
<tr>
<td>Collaboration</td>
<td>Collaboration</td>
<td>Networking</td>
<td>Cooperation</td>
</tr>
<tr>
<td>Networking</td>
<td>Networking</td>
<td>Networking</td>
<td>Merger</td>
</tr>
<tr>
<td><strong>Structures</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dyadic</td>
<td>Dyadic</td>
<td>Dyadic</td>
<td>Autonomous</td>
</tr>
<tr>
<td>Autonomous</td>
<td>Autonomous</td>
<td>Autonomous</td>
<td></td>
</tr>
<tr>
<td><strong>Extent of engagement</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strategic/Specific</td>
<td>Specific</td>
<td>Specific</td>
<td>Specific</td>
</tr>
<tr>
<td>Specific</td>
<td>Strategic</td>
<td>Strategic</td>
<td></td>
</tr>
</tbody>
</table>

For example, in New Zealand, coordination was actively encouraged and used to ensure delivery of cooperation, coordination and collaboration between—and within—the intelligence and law enforcement communities. Meanwhile, in Denmark with its long history of cooperative engagement, the government put in place programs, strategies and action plans

---

22 Listed from highest to lowest percentage of relationship identifications shown in the case studies.
23 The NZ Government results exclude central agency data, presenting only government data results.
that required cooperative approaches (for example, see Government of Denmark, 2009, 2011; Karlsson, 2012, p. 39). While in Finland, with its national focus on preparedness and comprehensive security concepts (Prime Minister’s Office, 2012), specific legislation was enacted that required the police (which included the domestic security intelligence service) and other law enforcement agencies to formally cooperate, coordinate and collaborate (Finnish Police, 2011, p. 8). Examples, it is contended, of Brodeur’s (2007) blending of high and low policing, and of Bigo’s (2000, pp. 171–172) concept of “securitization” and the blurring of the internal and external.

Finally, with regards to relationship types, Table 5.5 illustrated that the governments of the three countries had opted to focus their relationship efforts on the cooperation, coordination, and collaboration settings on the RC (see Figure 2.1). There appeared to be less appetite amongst those governments for the use of autonomy, networking, or mergers. That deliberate selection of relationship types, it was contended, fitted ideally with the next finding regarding the structures that the governments’ desired.

When it came to the structures that the governments sought to support inter-organisational relationships, it was clear from the case studies that networked arrangements were preferred when it came to responses to “wicked” issues, such as transnational smuggling, terrorism, and cyber threats. That finding fitted with the concept of “security networks” as discussed by various scholars, and described by Dupont (2007) and Whelan (2015, pp. 1–2). The networks identified in the research spanned a range of settings from both “high” policing (for example: organised transnational crime and terrorism) to “low” policing (for example: local crime prevention) environments (Whelan, 2015, pp. 1–2). The approach also fitted with Dupont’s view (2007, p. 77) that networks were used by governments to address the fragmentation in their systems that arose from the financial crisis they encountered in the 1970s which resulted in divestment of particular activities.

In delivering policy responses, the governments studied also showed that they desired their intelligence and law enforcement agencies to focus on dealing with specific issues and tasks (Table 5.5). However, the findings did confirm that some strategic engagement was occurring between operational agencies and policymakers, particularly in situations where governments wanted the development of programs, strategies and action plans to have multi-agency input.

As a means of demonstrating that point, in preparing policies Denmark and Finland were particularly active in the use of multi-agency working groups and steering committees at ministerial, senior official, and operational levels (see Department of Gender Equality, 2007, pp. 9–10; Ministry of the Interior, n.d., Ministerial working groups), while New Zealand continued to demonstrate use of the central agencies to coordinate the development of their responses. In doing so New Zealand also made use of working groups in ways similar to their Nordic counterparts (see Ministry of Business, Innovation & Employment, 2013, p. 7; New Zealand Security Intelligence Service, 2008, p. 12). These approaches were consistent with earlier research concerning networks (including security networks), and in particular their governance (Dupont, 2007, pp. 77–78). As explained by Provan and Kenis (cited in Whelan, 2015, p. 4), a network’s activity can either be “brokered through a central actor or lead organisation” (hub-design) (2015, p. 4) as was the case in the New Zealand approach, or alternatively, governance can be “shared” which sees all concerned taking ownership. The
shared model appeared to best fit the approach most often taken in the Danish and Finnish environments.

In exploring Dupont’s (2007) discussion of security networks further, it was evident that all three countries were engaging (to greater or lesser degrees) in creating what he described as “institutional networks” (2007, p. 80) in response to transnational criminality. Those institutional security networks, while primarily focused on addressing specific issues (such as illegal migration or terrorism) and offering the best means of assessing and preventing or responding to risk (2007, p. 78), also provided, it was argued, links to the cross-border networks, what Dupont (2007, pp. 80–81) labelled “international security networks,” enjoyed by the parties to the institutional network. International security networks crossed borders and linked agencies within one state to like-focused agencies in other states, or to organisations or arrangements especially constructed to facilitate cooperative activities (2007, pp. 80–81), for example Interpol—for police, or the Club of Berne—for security and intelligence agencies. Thus the links to international security networks, with their beyond-the-border access to information and intelligence, potentially provided a ‘multiplier’ effect to the jurisdiction-bound institutional security networks revealed in the research.

The above discussion, it is argued, is directly consistent with Bigo’s (2000, p. 171) commentary on the shift in the security environment towards “securitization”. Securitization being that state of affairs resulting when the internal and external search for “enemies” or “common threats” converges from what were once quite separate and distinct disciplines as a result of “merging and de-differentiation” (2000, pp. 171—172) into a “justification for new structures and more cooperation between agencies.”

Underpinning the development of policy responses resulting in the new structures and cooperation, and empowering the mechanisms used, each of the case study countries ensured legislation permitted inter-organisational relationships to occur. Finland, with its cooperation legislation displayed that trait in a unique way (see Act on Cooperation between the Police, Customs and Border Guard (687/2009) (FIN)), while Denmark and New Zealand provided permissive organisational legislation that ensured agencies could work in a cooperative fashion (see Policing Act 2008 (NZL); Politi-loven 444/2004) (DEN)). Moreover, it was identified that the governments studied empowered their agencies to expand cooperation beyond its strict dictionary definition into collaborative arrangements, such as those involving creation of multi-agency assessment and intelligence units or establishment of joint-agency task forces to tackle particular forms of transnational criminality (see Persson, 2013; Walsh, 2011; Danish National Police, n.d. (b), p. 9; Act on Cooperation between the Police, Customs and Border Guard (687/2009) (FIN)).

But permissive legislative environments were not the only way relationships in the case studies were nurtured. The governments involved also used encouragement to ensure cooperative networks occurred. Encouragement came in the form of ministerial pronouncements and government programs, strategies, and action plans that included the description of, and requirement for, multi-agency engagement (see Government of Denmark, 2009, 2011; Ministry of the Interior, 2008a; King, 2008). The programs and plans referred to often-included high-level steering groups (at ministerial and/or senior official level) to monitor implementation and delivery effectiveness, while the initial policy development
phase regularly involved multi-agency working groups at operational level, and occasionally engagement with private sector and not-for-profit actors.

Overall, the government expectation findings established that the case study countries were aligned with several of the main findings from the security reviews undertaken by others in the early 2000s (see Flood, 2004; Kean et al., 2004; Murphy et al., 2006). Those findings included confirmation that “wicked” issues—which spanned multi-agency mandates, and showed no cognisance of traditional foreign/domestic responsibility divides—needed horizontally coordinated, cooperative (and/or collaborative), networked, multi-agency efforts in response, as is well documented by scholars, including those who have researched and written about security networks (Whelan, 2012 and 2015).

Intelligence Community Relationships

In general terms, development of inter-organisational relationships between agencies in the intelligence and law enforcement communities faced a number of challenges. Issues, such as secrecy, need-to-know information sharing (or non-sharing), compartmentalisation, and cultures, built on historic foreign verses domestic divides were entrenched (Aldrich, 2011, pp. 26 & 32; Bamford, 2004, pp. 750–751; Hoffman, 2010, p. 46; Lowenthal, 2012, p. 49; Persson, 2013, pp. 16–17; Svendsen, 2008, pp. 663–664; Zegart, 2007, pp. 68 & 112–113). Traditional bureaucratic arrangements also played a part in shaping how relationships were formed and used. For instance, in Denmark and Finland the intelligence arrangements were quite different to New Zealand, with the domestic security services still being integral parts of the respective national police organisations (Finnish Police, n.d., n.d.; Weller, 2000, p. 172). Furthermore, in Denmark and Finland the foreign intelligence services were elements of the military establishment (see Danish Defence Intelligence Service, 2013), while in New Zealand, the domestic security intelligence service and the foreign-focused signals intelligence bureau were both civilian agencies operating pursuant to their own specific statutes.

Despite those challenges and differences, the three case studies showed that inter-organisational relationships had been formed, as shown below in Table 5.2. Each study confirmed intelligence engagement with law enforcement, and between the different intelligence services where those existed. Furthermore, collaboration was also evident through the formation of small, niche units working on tasks such as threat assessment, counter-terrorism, non-proliferation of weapons, and money laundering. That finding supported the view formed by Brodeur (2005, p. 805) that a “converse awareness” had developed acknowledging “security and intelligence services should play an increasing part in law enforcement.”

When it came to the structures supporting the intelligence communities (IC) relationships (Table 5.2), data from Finland and New Zealand identified a mixture of networked and dyadic arrangements were occurring. Denmark’s findings, however, still showed a distinct leaning towards dyadic engagement by its intelligence services. That said, there was data confirming the emergence and growth of networked arrangements in the Danish environment. The Center for Terror Analysis, hosted within the security service, was one such example, while the security service’s engagement with the Money Laundering Secretariat and the national police’s Task Force East were also illustrative of networked relationships.
With little data found about the Danish and Finnish foreign intelligence services it was more difficult to determine the structures underpinning relationships regarding that side of the community. However, in Denmark, emphasis on implementing the recommendations from the intelligence services’ benchmarking reports, and acknowledgement from senior officials that threats now crossed borders (geographic and bureaucratic), suggested progress was being made on dismantling historic domestic/foreign divides (and associated political silos) still evident in data from some Danish sources (see Tebbit, 2006; Anonymous British Security Service Officer, 2006).

Table 5.2. IC inter-organisational relationship comparisons

<table>
<thead>
<tr>
<th>Relationship continuum + 1</th>
<th>Denmark</th>
<th>Finland</th>
<th>New Zealand</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Relationship types</strong></td>
<td>Cooperation</td>
<td>Cooperation</td>
<td>Cooperation</td>
</tr>
<tr>
<td></td>
<td>Collaboration</td>
<td>Collaboration</td>
<td>Collaboration</td>
</tr>
<tr>
<td></td>
<td>Coordination</td>
<td>Coordination</td>
<td>Networking</td>
</tr>
<tr>
<td><strong>Structures</strong></td>
<td>Dyadic</td>
<td>Networked</td>
<td>Networked</td>
</tr>
<tr>
<td></td>
<td>Networked</td>
<td></td>
<td>Dyadic</td>
</tr>
<tr>
<td><strong>Extent of engagement</strong></td>
<td>Specific</td>
<td>Specific</td>
<td>Specific</td>
</tr>
<tr>
<td></td>
<td>Strategic</td>
<td>Strategic</td>
<td></td>
</tr>
<tr>
<td><strong>Motivations</strong></td>
<td>Encouraged</td>
<td>Legislated</td>
<td>Encouraged</td>
</tr>
<tr>
<td></td>
<td>Voluntary/Legislated</td>
<td></td>
<td>Legislated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Voluntary</td>
</tr>
</tbody>
</table>

When it came to the extent of engagements within IC relationships, it was found they were primarily specific in nature with particular tasks and issues being worked on (Table 5.2). Although, in New Zealand, where central agency business units operated inside the IC—performing leadership roles—strategic engagement was taking place, particularly in regards to amalgamating the independent intelligence agencies in line with the new concept of “one community” (Whibley, 2013). Furthermore, the Danish case study also showed a small amount of data indicating strategic engagement by the Danish Security and Intelligence Service in raising threat awareness across sectors and in coordinating agencies with internal security responsibilities.

On the subject of motivation, the comparison (Table 5.2) showed that intelligence community relationships were motivated by all three of the identified drivers. Encouragement and legislation featured most prominently across the studies. Finland’s result, influenced by the _PTR Act (2009)_ showed the centrality of legislation to relationships in that country, while both Denmark and New Zealand relied in the first instance on encouragement for intelligence relationships to occur.

Overall, the three case studies revealed that each country’s intelligence community was engaging in relationships with their respective law enforcement counterparts. Those relationships involved cooperation, coordination, and collaboration, and in each case the relationships were in apparent recognition of the fact that new threats in the security environment crossed both national borders and agency mandates.

---

24 Listed from highest to lowest percentage of relationship identifications shown in the case studies.
Law Enforcement Community Relationships

The comparison of the law enforcement communities’ relationships in Table 5.3 confirmed engagement with intelligence counterparts was occurring, and that in the majority of instances those relationships involved cooperation, coordination, and collaboration (see RC, Figure 2.1). Interestingly, the comparison showed that coordination was the relationship type most often identified in Denmark and New Zealand, from the law enforcement perspective. A possible reason for that prominence was assessed to be that law enforcers, with their public profiles and mandates, which encompassed a variety of “wicked” issues, were considered the appropriate agencies to have in coordination roles, while intelligence agencies, with their lower public profiles and narrower organisational focuses, were more suited to supporting roles (for example, see Brodeur, 2010, pp. 222–223 for discussion of the respective “occupational and organizational” of a police and security intelligence organisation).

The second interesting observation arising from Table 5.3 was the identification of collaboration as the next most prominent relationship type for Denmark and New Zealand. That result was contributed to through the use of multi-agency task forces to tackle transnational criminal activity, and the involvement of law enforcement in niche units targeting specific issues and tasks, the same as those detailed above regarding the intelligence community. That finding for Denmark was different to the one observed with regards to the Danish IC. The finding was assessed as being indicative of the more traditional approaches to relationships taken by the intelligence agencies as alluded to in the Danish intelligence services’ benchmarking reports (Tebbit, 2006; Anonymous British Security Service Officer, 2006).

Table 5.3. LEC inter-organisational relationship comparisons

<table>
<thead>
<tr>
<th>Relationship continuum + 1</th>
<th>Denmark</th>
<th>Finland</th>
<th>New Zealand</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Relationship types</strong></td>
<td>Coordination</td>
<td>Cooperation</td>
<td>Coordination</td>
</tr>
<tr>
<td></td>
<td>Collaboration</td>
<td>Coordination</td>
<td>Collaboration</td>
</tr>
<tr>
<td></td>
<td>Cooperation</td>
<td>Collaboration</td>
<td>Cooperation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cooperation</td>
<td>Collaboration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Autonomy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Networking</td>
</tr>
<tr>
<td><strong>Structures</strong></td>
<td>Networked</td>
<td>Networked</td>
<td>Networked</td>
</tr>
<tr>
<td></td>
<td>Dyadic</td>
<td>Dyadic</td>
<td>Dyadic</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Autonomous</td>
</tr>
<tr>
<td><strong>Extent of engagement</strong></td>
<td>Specific</td>
<td>Specific</td>
<td>Specific</td>
</tr>
<tr>
<td></td>
<td>Strategic</td>
<td>Strategic</td>
<td>Strategic</td>
</tr>
<tr>
<td><strong>Motivations</strong></td>
<td>Legislated</td>
<td>Encouraged</td>
<td>Encouraged</td>
</tr>
<tr>
<td></td>
<td>Voluntary</td>
<td>Legislated</td>
<td>Legislated</td>
</tr>
<tr>
<td></td>
<td>Encouraged</td>
<td></td>
<td>Voluntary</td>
</tr>
</tbody>
</table>

Moving on to the comparison of structures in Table 5.3, networks were most commonly used by law enforcement in each case study country. That finding was consistent with the desires of the governments concerned, and of the structures involving the intelligence/security agencies in Finland and New Zealand. Equally clear was that specific engagement on issues and tasks led when it came to the extent of engagement in law

---

25 Listed from highest to lowest percentage of relationship identifications shown in the case studies.
enforcement relationships (Table 5.3). Again, that was consistent with the governments’ desires and the intelligence community’s engagement results.

As a final point, with regard to the motivation of relationships (Table 5.3), all three motivational types were evident, with encouragement and legislation having greater prominence than voluntary arrangements. That outcome led to the view forming that for law enforcement agencies to engage in inter-organisational relationships, governments needed to ensure that the legislative environment was permissive, and that the governments actively encouraged relationship activity.

It was evident that the three law enforcement communities in the studies were aligned with the expectations of their respective governments. They were engaging in relationships with their intelligence counterparts. They were using networked structures, and focusing their activities on specific boundary-spanning issues and tasks. Again, as with the intelligence communities, it was assessed that the governments involved needed to provide a permissive legal environment and visible encouragement for those relationships. That encouragement, it was found, came primarily through the introduction of programs, strategies and action plans that necessitated relationship interactions.

**Policy and Practice Benchmarks and Implications**

Before embarking on consideration of the policy and practice benchmarks and implications arising from the above comparisons, it was felt appropriate to locate and consider additional comparative knowledge regarding the three case study countries with reference to, if possible, the impact of “wicked” policy issues and how they addressed them. Because this study did not address the issue of effectiveness regarding the approaches taken by the case study countries, it was considered relevant to attempt to situate the three countries in a global context with respect to how their approaches to governance and bureaucratic challenges were viewed. In doing so the perceived ‘usefulness’ of the policy and practice benchmarks presented later could be viewed against that context.

Research identified three publicly available indexes that ranked countries against various indicators, a number of which, it was posited, had relevance to case study countries responses to “wicked” policy issues like transnational criminality.

The first indexes identified were the Global Peace Indexes prepared annually by the Institute for Economics and Peace (IEP) (Institute for Economics and Peace, 2012, p. 3). The institute described itself as an “independent, non-partisan, non-profit research organisation” which was accredited to the United Nations as a non-governmental organisation (2012, p. 2). The Global Peace Indexes reviewed for the study covered the years 2008–2012. The indexes were compiled using sets of indicators (24 in 2008 and 23 for the remaining years) to determine the ranking of countries based around “three broad themes: the level of safety and security in society; the extent of domestic or international conflict; and the degree of militarization” (Institute for Economics and Peace, 2008, p. 2, 2012, p. 3). Those themes enabled the measurement of what the institute, citing Galtung (2012, p. 69), termed “negative peace,” or as Galtung was quoted as stating “the absence of violence” and the “absence of the fear of violence” (2012, p. 69).

The Global Peace Index rankings for the three case study countries over the period 2008–2012 are shown in Table 5.4.
Table 5.4. Global Peace Index rankings for case study countries

<table>
<thead>
<tr>
<th>Country</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denmark</td>
<td>2*</td>
<td>2</td>
<td>7</td>
<td>4</td>
<td>2**</td>
</tr>
<tr>
<td>Finland</td>
<td>8</td>
<td>9</td>
<td>9</td>
<td>7</td>
<td>9</td>
</tr>
<tr>
<td>New Zealand</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2**</td>
</tr>
<tr>
<td><strong>Total</strong>*</td>
<td>121</td>
<td>144</td>
<td>149</td>
<td>153</td>
<td>158</td>
</tr>
</tbody>
</table>

(*score of 1=most peaceful; **shared ranking; ***number of countries assessed each year)

In 2012, the institute expanded its research and focus to include not just the concept of negative peace (as represented in the Global Peace Indexes) but also Galtung’s second dimension that he termed “positive peace” (Institute for Economics and Peace, 2012, p. 69). Positive peace was described as being “derived from preventative solutions which are optimistic and facilitate a more integrated society” (2012, p. 69), with the overall outcome being “cooperation for mutual benefit, and where individuals and society are in harmony” (2012, p. 69). The institute, therefore, developed a methodology to assess and report on positive peace through use of 21 indicators across eight domains (2012, p. 69). Two of the eight domains were assessed to be of relevance to this study, with one being “well-functioning government” and the other “low levels of corruption” (2012, pp. 74 & 79). The positive peace indicator results achieved for the two relevant domains, and the institute’s overall ranking after assessment of 108 countries, with regards to the case study countries (2012, pp. 80 & 84), are shown in Table 5.5.

Table 5.5. Positive Peace Index rankings for case study countries

<table>
<thead>
<tr>
<th>Countries</th>
<th>Overall rankings* (1–108)</th>
<th>Well-functioning government**</th>
<th>Low levels of corruption**</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denmark</td>
<td>4</td>
<td>1.02</td>
<td>1.02</td>
</tr>
<tr>
<td>Finland</td>
<td>3</td>
<td>1.00</td>
<td>1.21</td>
</tr>
<tr>
<td>New Zealand</td>
<td>9</td>
<td>1.22</td>
<td>1.01</td>
</tr>
<tr>
<td><strong>Total countries</strong></td>
<td><strong>108</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(*1=most positive peace indications; **ranking range: 0.0 (more positive peace) to 5.0 (less positive peace))

The data used by the Institute for Economics and Peace (IEP) to assess the levels of corruption came from two sources: the World Bank’s Governance Indicators Control of Corruption Measure, and Transparency International’s Corruption Perceptions Index (Institute for Economics and Peace, 2012, p. 79). Since Transparency International’s Corruption Perception Index also independently ranked countries, the case study countries results for the

---

years 2007–2012 were located and are shown in Table 5.6 (Transparency International, n.d. (a)–(f), n.d.).

Table 5.6. Corruption Perception Index rankings for case study countries*

<table>
<thead>
<tr>
<th>Countries</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denmark</td>
<td>1**</td>
<td>1**</td>
<td>2</td>
<td>1**</td>
<td>2**</td>
<td>1**</td>
</tr>
<tr>
<td>Finland</td>
<td>1**</td>
<td>5</td>
<td>6</td>
<td>4</td>
<td>2**</td>
<td>1**</td>
</tr>
<tr>
<td>New Zealand</td>
<td>1**</td>
<td>1**</td>
<td>1</td>
<td>1**</td>
<td>1</td>
<td>1**</td>
</tr>
<tr>
<td><strong>Total</strong>*</td>
<td>180</td>
<td>180</td>
<td>180</td>
<td>178</td>
<td>183</td>
<td>176</td>
</tr>
</tbody>
</table>

(*ranking of 1=perception of least corrupt; **shared ranking; ***number of countries and territories assessed each year)

Transparency International, similar to the IEP, described itself as a politically non-partisan organisation that placed great importance on its independence. It stated on its website that it “works with partners in government, business and civil society to put effective measures in place to tackle corruption” (Transparency International, n.d. (g), n.d.).

The third and final report to be considered in respect of additional context was the 2012 Global Terrorism Index—also produced by the Institute for Economics and Peace (Institute for Economics and Peace, n.d.). That document sought to “build a thorough picture of the impact of terrorism over a 10-year period” (n.d., p. 6). To create the index the IEP relied upon “data from the Global Terrorism Database … collected and collated by the National Consortium for the Study of Terrorism and Responses to Terrorism …” (n.d., p. 6). The National Consortium’s dataset contained data about 104,000+ terrorist events worldwide (n.d., p. 6). The case study countries index results are shown in Table 5.7.

Table 5.7. Global Terrorism Index rankings for Case study countries – 2012

<table>
<thead>
<tr>
<th>Countries</th>
<th>Rankings* (1–116)</th>
<th>Score** (10–0)</th>
<th>Terrorism events - 2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denmark</td>
<td>77</td>
<td>1.129</td>
<td>1</td>
</tr>
<tr>
<td>Finland</td>
<td>107</td>
<td>0.069</td>
<td>0</td>
</tr>
<tr>
<td>New Zealand</td>
<td>104</td>
<td>0.079</td>
<td>0</td>
</tr>
<tr>
<td><strong>Total</strong>**</td>
<td>158</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(*1=most impacted by terrorism; **10=most impact of terrorism; ***recorded as occurring in the case study countries; ****number of countries assessed)

It must be acknowledged that none of the above listed rankings and scores have been causally linked to the inter-organisational relationship settings or mechanisms used by the case study countries. However, the rankings achieved by the three countries are likely to be coveted by countries that fell short of attaining such results. In achieving the rankings and scores outlined, the case study countries have been, it was argued, identified as similar in additional respects over and above the original parameters used for case study selection. Moreover, it was posited, that the case study countries are ones whose approaches to tackling “wicked” issues are at least worthy of consideration by countries aspiring to rank as well in the indexes referred to.
That said, when the findings from the comparisons of the three case study countries were considered alongside the earlier findings in this study regarding scholarly views on inter-organisational relationships (see earlier discussion at pages 15–21), it became apparent that four distinct environmental elements were discernible across the case studies. Those four elements were deemed to be necessary if governments and/or organisations desired inter-organisational relationships mirroring those evident in Denmark, Finland, and New Zealand. The four elements were given the broad labels: Permission, Leadership, Flexibility, and Adaptability. Supporting those four environmental elements were three equally distinct RC selections. Those selections related to the particular relationship types chosen (namely cooperation, coordination, and collaboration), the use of networks to support those choices, and finally the primary focus on specific issues and tasks when it came to the extent of engagement being entered into. Each of these elements and choices are discussed below, commencing with permission.

The three case studies identified that the legislative environments in each of the countries expressly permitted inter-organisational relationships. In Denmark and New Zealand permission was built around the concept of cooperation, but relationships were permitted to expand to include coordination and collaboration. In Finland, permission was taken further through the enactment of the PTR Act (2009), which, while labelled as a cooperation mechanism, also empowered coordination and collaboration between the three agencies it related to. Beyond the enactment of legislation in 2009, Finland continued to work on ensuring legislative permission via a Parliamentary Committee tasked to “identify legislative and institutional barriers to inter-ministry mobility” (Organization for Economic Cooperation and Development, 2015, p. 14). Legislative permission, it was argued, set the foundation for all of the subsequent inter-organisational relationship activities identified in the case study countries.

Beyond legislative permission, reflection on the case studies gave rise to the view that there were two further interlinked forms of permission present and conjoined with the legislative. The second forms of permission came from governments actively encouraging relationships or, to draw upon Severance’s contention (2005, p. 23), embedding an “underlying virtue of unity of effort.” Government encouragement observed in the case studies was conceived of as delivering Dalgaard-Nielson’s (2006, p. 4) “… culture of cross-government cooperation.” In the case studies, that encouragement was provided by way of speeches and media releases emanating from government leaders and ministers. It also came through the policies, programs, strategies and actions plans that the three governments implemented, which necessitated inter-organisational relationships to form and operate. Government permission was also evident through mechanisms, like ministerial working groups in Denmark, Parliamentary Committees in Finland, and central agency-led horizontal coordination in New Zealand, which drove increased inter-organisational relationships.

The third form of permission, viewed as implicit and closely linked to that of the governments, was societal permission. That concept involved the citizens of the three countries giving tacit approval to the inter-organisational relationships encouraged by their governments. The tacit approval observed during the case studies arose through the three governments signalling their inter-organisational relationship expectations via speeches, media releases, and publicly accessible policy documents, and in response, those signals not
eliciting wide spread public disapproval or backlash (for example Denmark’s Action Plan to Combat Human Trafficking, Finland’s PTR Act (2009) legislation, and New Zealand’s National Security System document). Societal permission was similar in concept to Rudner’s (2010, p. 139) “security culture” concept, wherein he posited that the “sustainability of any system of national security in a democracy depends … on building and maintaining public confidence in the necessity, propriety and efficiency of the national security machinery being deployed.”

A singular example of the risk associated with societal permission (beyond the international examples linked to Edward Snowdon’s disclosures) occurred in New Zealand during the period of that case study. It centred on operational support provided by the country’s signals intelligence agency to the New Zealand Police in regards to a high-profile extradition case. The case arose in late 2011, and developed an increasingly notable media profile through 2012 and 2013 as the New Zealand Government and the agencies involved endeavoured to manage the repercussions from it (see Key, 2012; New Zealand Intelligence Community, 2015; Rogers, 2015). The case ultimately required the New Zealand government to amend legislation to clarify the intelligence agency’s relationship permissions and to dampen public anxiety about intelligence/law enforcement relationships. The case also resulted in the adoption of new and improved protocols by the agencies involved covering how they would work together in the future (Key, 2012), again to placate the public and re-establish societal permission for their relationship.

Permission, however, was just one of the elements identified, and the case studies revealed that it was not relied upon solely to nurture inter-organisational relationships. The second element identified from across the studies was visible leadership. The agencies examined had their leaders (more often than not) visibly engaged in the inter-organisational relationship process. That engagement occurred through membership of horizontal coordinating mechanisms, such as high-level committees (i.e. New Zealand’s ODESC), or through involvement in multi-agency steering groups (i.e. Finland’s National Plan of Action against Trafficking in Human Beings). In the case studies, visible leadership engagement (or “leadership commitment” as it was termed by New Zealand’s State Services Commission (2008, p. 11)), and the means used to facilitate it, appeared to establish a deliberately observable bridge between the setting of policy and its operational implementation. The second aspect of visible leadership observed related to the alignment of organisational values and mission statements, and internal culture, to inter-organisational relationships.

Organisations deliver messages to their staff and others by way of their values and mission statements, and through the culture existing within the organisation (Brodeur, 2010, p. 194; Dalgaard-Nielsen, 2006, p. 8). Examples in the case studies indicated that alignment of those messages helped to publicly ‘set the stage’ for what the organisations expected and desired (see Finland’s border guard’s vision and values statements, Rajavartiolaitos, 2012, p. 28; New Zealand’s “Safer Communities Together” New Zealand Police, 2008, p. 2). However, reframing written statements about values and missions may prove easier than re-setting organisational cultures as Dalgaard-Nielsen suggested in his paper on civil-military cooperation in Denmark (2006, pp. 8–10) and as Brodeur (2010) discussed in his submission to the Canadian commission of inquiry into the bombing of Air India flight 182. Misalignment of messages can cause confusion amongst those charged with implementing policies
requiring inter-organisational relationships. Those misalignments can have profound impacts as Brodeur (2010, pp. 192–193) detailed in his paper submitted to the Air India commission of inquiry.

The last two elements discerned from the case studies that support inter-organisational relationships were less obvious, but were, it was argued, nonetheless present and necessary for the identified relationships. Two words used by Dupont (2007, p. 80) to describe the attraction of networks—flexibility and adaptability—were adopted to describe those elements. One of those elements occurred at the organisational level and was labelled flexibility. The concept of flexibility appeared to be similar to Lawrence and Lorsch’s contingency theory of organisational adaption as cited in Axelsson and Axelsson (2006, p. 76). The need for organisational flexibility (regarding human resources) was also raised by Murdoch (2009, pp. 5–9) during his review of New Zealand’s intelligence community. From the case studies it was evident that the organisations examined demonstrated flexibility by accepting and, when necessary, adjusting (sometimes in major ways, such as working in a co-location setting with a number of counterpart entities) to the changed operating environments arising from policies aimed at breaking down bureaucratic silos and countering departmental fragmentation regarding the delivery of responses to “wicked” security issues.

Flexibility was evident despite Brodeur’s (2005, p. 801) contention that “security and intelligence services are conservative organisations that do not quickly adapt to change.”

Flexibility was evident despite Brodeur’s (2005, p. 801) contention that “security and intelligence services are conservative organisations that do not quickly adapt to change.” It was contended that the flexibility observed in the case studies was acknowledgement by the agencies involved of the need to adjust to new risks resulting from the very public opening of Birkland’s policy window brought about by the terrorist events of the early twenty-first century (Birkland, 2004, p. 189), the speed with which modern crises can develop and impact countries (Scott, 2014), and other challenges to the established “world order” (Whibley, 2013, p. 1).

The resulting new operating environments across the case study countries encouraged joined-up, multi-agency working arrangements (security networks), which in turn required flexibility in organisational structures, cultures and reporting lines (see Denmark’s Task Force East—Danish National Police, n.d. (b), p. 9, and State Prosecutor for Serious Economic Crime, 2011, p. 11; and Finland’s Internal Security Programme—Ministry of the Interior, 2008a). Those changes also involved organisations in joint planning and implementation arrangements with other government (and sometimes non-government) agencies, resource sharing (including people), working in co-located environments, and occasionally having to give up organisational turf to work in collaborative units, such as multi-disciplinary teams or task forces (see New Zealand’s Organised and Financial Crime Agency arrangements—New Zealand Police, 2008, p. 16).

The second less obvious element emerging from the cases concerned the people working in the organisations studied. The label given to the people element was adaptability. Like their organisations staff were required to adapt to working arrangements that saw them

---

27 On the subject of adapting to change, New Zealand’s Performance Improvement Framework review of its core intelligence community agencies supported Brodeur’s contention. Whilst adapting to some of the changes imposed from 2010 onwards, in 2014, the community was identified as still not having overcome the cultural challenge of collaboratively working together (Bushnell & Wilson, 2014, pp. 14–15).
engaging in multi-agency groups and multi-disciplinary teams, as in the examples provided above. The case studies all contained examples of such arrangements, with perhaps one of the most ambitious being New Zealand’s move away from independent and physically separate intelligence agencies into a “one community” concept, housed in a single building (Whibley, 2013).

A change, such as the one New Zealand embarked upon, required people to not just work for their home agency, but to also contribute toward a new and combined greater good (Scott, 2014). That contribution was made through new multi-disciplinary arrangements involving people from different organisational cultures and reporting lines mixed together to engage in new collaborative endeavours (Scott, 2014). Those impositions, it was posited, required the people impacted to display adaptability if the policies involved were to be implemented and, at the individual level, if they were to continue working in the new environment. Adaption, however, was not guaranteed, nor simple to achieve; for example, a review of New Zealand’s new ‘one community’ working arrangements in 2014 revealed that not everyone had adapted as hoped. The performance review (Bushnell & Wilson, 2014, pp. 14–15) found continued evidence of lack of mutual respect and trust between staff from the various organisations that made up the new joint arrangements. Whelan (2015) also discussed at length the challenges present in security networks for people from different organisational cultures (or sub-cultures) who have to work together towards common outcomes.

With regards to the interplay between the four elements and inter-organisational relationships, Figure 5.1 was developed as a visual representation of the above discussion. In the figure, three organisations (A, B, and C) portray inter-organisational relationships. For a dyadic (A + B) or networked relationship (A + C + B) the four elements need to be present either across the general environment (permission), or within each of the participating organisations (leadership, flexibility, and adaptability). If, for example, A’s legislation prohibited the sharing of the information it gathers (i.e. ‘A’ lacked a specific legislative permission to share), its ability to work with B or C is compromised. Alternatively, if B’s leadership rejected the need to work with others (either openly, or implicitly—which may be more likely in a bureaucratic environment), then its ability to work with A or C is also compromised.

It must be stressed though that the presence of the four elements alone does not guarantee the success of relationships (see Bushnell & Wilson, 2014 with regards to New Zealand, and Agbonlahor, 2015a with regards to Finland). Success, it was posited depends upon factors other than just those identified by this study (for example, the need for trust between the parties to a relationship, see Himmelman, 2002, p. 1; Huxham, 2003, pp. 408–409; Whelan, 2012, p. 4). However, it was further posited, that those other factors were suspected of being linked to the factors that this study has highlighted.

Having articulated the four elements that emerged from consideration of the case studies, what connection, if any, did those elements have to policy or practice? The answer arrived at was that the elements themselves were the policy and practice benchmarks a government would need to take account of if it aspired to replicate the approaches taken in the case study countries.

For example, the start point for a government desiring effective intelligence and law enforcement inter-organisational relationships would be consideration of the country’s
permission environment. Does legislation allow agencies to lawfully work together? And, linked to that question, how is government through its actions supporting (or going to support) such relationships? Finally, with respect to permission, the government should also be attuned to the public mood when it comes to inter-organisational relationships between intelligence and law enforcement agencies. Importantly, is there support for such arrangements, or are they likely to raise anxiety amongst the citizenry? Beyond the earlier example of societal anxiety arising in New Zealand, Canada also provided an interesting historical example of societal anxiety concerning intelligence and law enforcement interaction (O’Connor, 2006b, pp. 3234). That situation arose from the Royal Canadian Mounted Police’s dual role as both security intelligence agency and police organisation in the late 1970s and early 1980s. That anxiety (or lack of trust as it was characterised) (2006, p. 34), and other issues, ultimately gave rise to the separation of the two functions in the mid-1980s and the formation of the Canadian Security Intelligence Service.

Once the permission environment is considered favourable (or being managed), the next benchmark to consider would be leadership. What mechanisms are in place, or can be put in place, to ensure visible leadership of inter-organisational relationship development? Visibility applies to both what government can observe (to confirm commitment to the implementation of its policies), and what the people working within the affected organisations can see (to confirm that their leaders are committed and engaged in the process of policy implementation). For example, Whelan (2015, p. 11) in discussing security networks, cited Schein’s (2010) argument that forming an appropriate culture is first and foremost a “function of leadership, with leaders espousing the ‘correct’ ways of thinking and acting.” Visibility can also apply to the citizenry in the way Denmark, Finland, and New Zealand ensured public visibility of their inter-organisational relationship endeavours (see New Zealand’s National Security Strategy—Department of the Prime Minister and Cabinet, 2011b, and Agbonlahor, 2015b regarding New Zealand’s bureaucratic transparency). Finally, on the topic of leadership, are there vehicles available, such as committees or working groups (or both), that bring organisational actors together to further encourage dismantling of functional silos, building of “network culture” (Whelan, 2015, p. 11) and delivery of the inter-organisational relationship outcomes sought? In other words, the means by which “shared experiences” are created as Whelan (2015, pp. 11–12) discussed in his examination of security networks operating in the Australian environment.

Having considered the requirements associated with the first two benchmarks, the next one requiring attention relates to the organisations involved in the proposed relationship arrangements. The aim there would be to discover if they have (or can be empowered to have) the necessary flexibility to operate in the newly desired inter-organisational paradigm. That would require responsible government ministers and bureaucratic leaders confirming that the organisations (and they) had the required culture and capability to work within the relationship(s) envisaged by the policies they are charged with implementing. Traditional silos created by conservative organisations take time to dismantle, as Brodeur contended (2005, p. 801) and New Zealand’s intelligence community review confirmed (Bushnell & Wilson, 2014).

Nevertheless, the case studies showed it was possible to at least make a start towards delivering flexibility via structure and culture. That was evidenced through New Zealand’s
actions in creating its one community and introducing horizontal coordination to its wider public service (Whibley, 2013; Agbonlahor, 2015b); Denmark’s moves to improve relationships after its intelligence agencies benchmarking (Danish Security and Intelligence Service, 2010), and Finland’s Border Guard Strategy to 2022 with its focus on working cooperatively with law enforcement counterparts (Rajavartiolaitos, 2012).

The fourth and final benchmark to tackle is adaptability, or put another way, the ability of bureaucrats and other officials to adjust to their new cross-boundary work environments. Yan and Louis (1999, p. 38) discussed the additional demands placed on workers in such situations, or in what they termed “cross-functional teams.” Staff in such environments have to not only be capable of effectively undertaking their tasks, they are also required to “… bridge the boundaries of their functional–area ‘thought worlds’ … they must learn to listen across perspectives, to appreciate situations from disparate perspectives even as they build a common vision, language, sense of time and priorities” (1999, 38). Once again, organisations (and their people) need to demonstrate that they are capable of working effectively in those new arrangements. Do the organisations contain, or can they develop, leaders and staff who are comfortable and effective at working in cross-boundary (cross-functional) roles and settings?

The head of the State Services Commission in New Zealand, for example, claimed the country was investing in providing public sector leaders with “… an understanding of the environment that [they] are working within … [and] particularly giving our senior leaders different career paths that build a broader scale of experiences” with the stated aim of developing a “collective culture” (Scott, 2014) designed to “… force agencies to be working across the system rather that just within their own organisations” (Agbonlahor, 2015b). Meanwhile, Finland’s head of the Ministry of Finance, acknowledged that the country still had a way to go in achieving the same aim (Agbonlahor, 2015a), despite the positive picture painted by the documentary evidence referred to in the Finnish case study.

Enmeshed with the identified need to adapt to cross-boundary working is the issue of how all the parties involved (i.e. government, organisations, and workplace leaders) assess and reward (or sanction) those engaged in such activity? If organisations and the people in them are expected to work in multi-agency and multi-disciplinary settings what measures and indicators will be used to monitor their progress and identify successes (or failures)? At the governmental level, how can appropriate oversight and governance be applied to multi-agency inter-organisational activities to ensure their lawfulness (for example, see Harfield’s (2010) discussion of transnational criminal investigation governance). Furthermore, how will ministers’ reward (or sanction) agencies for successfully (or poorly) engaging with others when the results achieved sit squarely in the bailiwick of a particular minister’s responsibilities and not with the others involved? How do organisations do the same for the people involved in those endeavours?

New Zealand, it appeared, had attempted to tackle some of those issues with its “One Community, Many Agencies” intelligence initiatives (see New Zealand Intelligence Community, n.d., About Us). Joint Statements of Intent and budget submissions no doubt set about blending the various organisations’ contributions into a set of sector priorities and outcomes (see Department of the Prime Minister and Cabinet, 2012a, pp. 16–18); however, it remains to be seen if those processes flowed down into the organisational machinery
delivering intelligence outcomes. Separately, in regards to the wider public sector, reporting identified that the questions posed above were indeed exercising the minds of New Zealand’s central agency leadership. Both the state services commissioner and the head of the Treasury (Agbonlahor, 2015b; Scott, 2014) spoke about people and leadership issues when interviewed in recent times. They confirmed that re-connecting agencies and broadening leadership perspectives were paramount to better handling of complex, multi-mandate issues (Agbonlahor, 2015b; Scott, 2014). That awareness of what was important was, both went on to say, translated into greater focus on outcome and priority ownership with attendant governance settings.

An example of those governance settings was the creation of clusters of departmental chief executives around selected chief executives, whose roles were to deliver achievement of each of the government’s ten “better public service” ambitions (Agbonlahor, 2015b; Scott, 2014). While elsewhere, in regards to Finland, the Organization for Economic Cooperation and Development confirmed that ministerial bailiwicks were still a live issue. In the organisation’s report on Finnish governance it identified that the country still faced challenges in dismantling departmental stovepipes (Organisation for Economic Cooperation and Development, 2015, p. 77). It contended those stovepipes were being exacerbated by, amongst other things, “ministerial accountability for outcomes under their administrative sector budget” (2015, p. 77). Singapore appeared to offer some potential through both its “Reinvestment Fund” (Agbonlahor, 2015c) and planned career paths for senior civil servants (de Spiegeleire, 2013). The first of those concepts involved agencies bidding for contestable funds that were awarded to multi-agency projects that required “the concept of operating as one government, rather than simply as individual agencies” (2015c). While the second concept saw mid-level civil servants being deliberately cycled through a variety of roles in different government agencies so that when they come to occupy higher-level positions in the bureaucracy they brought a “whole-of-government” experience, attitude, and awareness to the processes they were involved in (de Spiegeleire, 2013).

Meanwhile, at the people level of inter-organisational relationships, joint-working arrangements will sometimes require staff to operate outside their parent organisation and away from its daily observation (see Persson, 2013, pp. 15–16). The work being undertaken by those staff may deliver results for one of the participant organisations rather than evenly to all (for example, see Harfield, 2008, pp. 494–495). Therefore, how can the contributions and experiences of the various staff involved be translated back into parent organisational understanding so the people involved are not disadvantaged (or over compensated) when it comes to advancement, remuneration or kudos? This study has not tried to explore those issues, but raises them as possible topics for future exploration.

Beyond the four elements discussed above, the RC dial choices identified earlier in the case studies are also particularly noteworthy from a policy and practice perspective.

Each of the case studies revealed the use of a combination (or blend) of cooperation, coordination, and collaboration when it came to inter-organisational relationship arrangements. While the primary choice varied (for example, coordination in New Zealand and cooperation in Denmark and Finland) the mix of the three types was common across each study. There was no evidence of serious use of, or reliance on, autonomy, networking or mergers when it came to inter-organisational relationships in the three countries.
The second choice from the RC dials evident in the studies was the use of networks to support the various inter-organisational relationships. That selection may well reflect the challenges provided by “wicked” policy issues like transnational crime, which spans multiple agency mandates and boundaries as discussed earlier. While some dyadic relationships remained in evidence, these appeared to be focused on specific legislated requirements—historical legacies—for example, supporting immigration agencies in determining the suitability of refugees or migrants for settlement—that were in the process of evolving into more contemporary arrangements that did involve networks.

The third and final RC dial choice of note from the case studies was that the majority of the inter-organisational relationships were setup to focus on and deal with specific tasks and issues, as opposed to strategic matters. While some strategic engagement was evident in collaborative relationships identified, most inter-organisational relationships in the case studies were targeted at quite specific policy matters.
Figure 5.1. Inter-organisational relationship elements
CHAPTER 6 — CONCLUSIONS

In examining the types of inter-organisational relationships existing between intelligence and law enforcement communities in Denmark, Finland, and New Zealand, the research has revealed that each country had recognised and responded to the two strategic themes posited at the start of this work. Those themes described the emergence of new threats that fail to acknowledge established notions of borders and sovereignty (thus blurring traditional domestic/foreign bureaucratic divides) and which, as a result, required effective inter-organisational relationships to counter them. The themes, in essence, defined the transnational criminality (wicked issue) nexus between government agency mandates and interests as described by Whelan (2012, p.54), and supported Brodeur’s (2005, pp. 799–805) contention that intelligence and law enforcement agencies—post-9/11 particularly—had a raison d’être for working more closely together.

In order to present a detailed examination of the three national responses, the research confirmed through review of the scholarly literature that organisations wishing to engage with others had a limited set of relationship options to choose from (see RC Dials, Figure 2.1). In describing those options, it was contended that once a relationship type had been selected, two further interlinked decisions were required. The first concerned what structure would support the selected relationship(s) (either dyadic or networked), while the second was about the extent of engagement the organisation desired to enter into (either strategic or specific). Associated with those decisions, and often necessitating them, the research defined and discussed the motives driving engagement in the first place. Was the organisation choosing to engage (voluntary), was it being encouraged by government, or required by legislation (or both) to do so?

Having described the range and constituent features of each inter-organisational relationship type (i.e. common, shared or distinctive features), the subsequent case studies confirmed a variety of identifiable inter-organisational approaches were used to respond to the “wicked” issue of transnational criminality, in the three separate, but similar, jurisdictions. The findings revealed that all three countries targeted their relationship arrangements around the cooperation, coordination, and collaboration settings on the RC (see Figure 2.1), with little appetite being displayed for autonomy or mergers. Networked, multi-agency engagement—via institutional security networks—was the leading support structure identified; with the extent of engagement being primarily focused on specific issues and tasks.

When the case study findings were aggregated to facilitate a cross-study perspective on the findings, it was contended that four distinct elements were highlighted as being necessary in the political and bureaucratic realms to foster inter-organisational relationships. Those elements were labelled: Permission, Leadership, Flexibility and Adaptability (see Figure 5.1).

Following on from confirming the four elements, policy and practice implications were identified for those wishing to replicate (or approximate) the inter-organisational approaches manifested in the case studies. On the policy front, it was concluded that government must ensure permissions are in place to empower the inter-organisational relationships it desires. The means available to deliver those permissions included specific
reference to relationships in legislation governing the operation of intelligence and/or law enforcement organisations (e.g. Denmark’s drafting of new legislation for PET and FE, or New Zealand’s legislation pertaining to New Zealand Police, NZSIS, and GCSB). Or, alternatively, a government could enact general legislation like Finland’s *PTR Act (2009)* that detailed how relationships between agencies shall be managed.

Government can also bolster the permissions it provides by actively encouraging the relationships it seeks. That encouragement can be in the form of ministerial working groups that oversee and steer the implementation of policies. Alternatively, encouragement can be provided by establishment of permanent horizontal coordination structures, such as New Zealand’s Officials Committee for Domestic and External Security Coordination (ODESC) arrangements, or through policy-by-policy approaches with the creation of high-level, issue specific, steering groups such as those used in Denmark and Finland.

Moreover, government needs to design and apply policies that require organisations to engage with each other in the style desired. So, government programs, strategies or action plans need to clearly articulate which RC settings the government desires (refer to Figure 2.1).

With regards to the practice implications arising from the research, it was concluded that organisations needed to prepare both themselves and their people (at all levels) for engaging in inter-organisational relationships. That preparation needed to ensure that members of the organisations’ executive leadership were visibly engaged in supporting inter-organisational relationships, as outlined in Severance’s unity of effort views (2005, p. 139), and also discussed by Whelan (2015, pp. 10–11). Membership of entities, such as multi-agency steering groups, or coordination committees (standing or ad hoc), provides the opportunity to deliver visible leadership and to develop a network culture. Moreover, linked to visible leadership, was the conclusion that the organisations needed to ensure that their stated values and mission, and internal culture (or the sub-cultures in specialist areas), supported their inter-organisational relationship ambitions.

Finland’s Border Guard organisation, for example, incorporated cooperation into its vision and organisational values statements (see Rajavartiolaitos, 2012, p. 28), while New Zealand’s Police identified that partnership was a key plank in its organisational strategy of achieving “Safer Communities Together” (see New Zealand Police, 2008, p. 2). Alignment of organisational position statements with relationship expectations also extends down to operational work groups. It was further concluded that if the operational levels of organisations did not also acknowledge the need for relationships, there was the potential for disconnect between the organisations’ expectations and the delivery of service by their relevant constituent parts.

On the subject of organisations’ constituent parts, they also provided the opportunity to identify situations and settings in which joint work can be engaged in, thus delivering on government expectations. Denmark’s Task Force East and New Zealand’s Counter-Proliferation Joint Section were examples of such niche opportunities. But the ability to successfully exploit those opportunities relied on the people within the organisation being adaptable to such changed working arrangements. It was concluded that the people side of the equation could not be left to chance.
Preparing organisations for inter-organisational relationships includes the management and development of their people. Do the organisations routinely assess people (during recruitment and promotion processes for example) on their ability to work constructively in multi-disciplinary teams, and to work in cross-boundary settings? Are experiential, educational, and training opportunities provided to staff, as discussed by Severance (2005, p. 140) and New Zealand’s state service’s commissioner (Agbonlahor, 2015b), thus enabling staff to: understand the need for inter-organisational relationships, appreciate the demands those relationships will make on them, and to experience the complexity of working within such arrangements? Short-term staff exchanges between organisations (Agbonlahor, 2015b; de Spiegeleire, 2013), regular multi-agency exercises (Kettl, 2003, p. 274; Severance, 2005, p. 140), and niche joint-operational activities such as fusion centres (Persson, 2013, pp. 15–17) provide inter-organisational relationship opportunities, particularly for staff identified as working on cross-boundary issues or those expected to be cross-boundary leaders and champions.

A further challenge arising from the use of networks—identified by scholars and arguably applying to each of the countries studied—concerned “accountability and evaluation mechanisms” (Dupont, 2007, p. 83; Harfield, 2010, p. 5). How are institutional security networks overseen and held to account when traditional means of doing so are structured to focus on particular organisations or their employees? That challenge was not explored in this research, but as early as 2000 Shearing (cited in Dupont, 2007, p. 83) had suggested the creation of a “policing board instead of a police board.” While elsewhere, in Australia for example, the Flood review (2004, p. 61) into the Australian Intelligence Community recommended the establishment of a Foreign Intelligence Coordination Committee. The suggested committee would bring together the heads of the intelligence agencies, along with the heads of the Australian Federal Police, Department of the Prime Minister and Cabinet, Defence and Foreign Affairs & Trade (2004, p. 61). One of the proposed functions of the committee was the “consider[ation of] cross-community issues including intelligence policy, capability development and resources.” Therefore, concepts and models exist that provide opportunity for scrutiny in response to the identified challenge.

In terms of acknowledging the limitations regarding this research, the most obvious one was the extensive use of publicly available secondary sources, the majority of which were gathered from government websites and consisted of official documents. Those sources were clearly prepared by their authors with particular agendas in mind and for specific audiences. Efforts were made to supplement those sources with other reporting from the media or scholarly texts, and in some instances those efforts were successful. Whilst use of secondary sources gave rise to potential weakness in the data, their use also gave rise to potential strengths, such as those outlined by Yin (2009, pp. 101–113) including: stability, unobtrusiveness, exactness, and coverage.

The use of an expert panel, consisting of people who lived and worked in the case study countries, was designed to address the limitations discussed above and others. Review by the expert panel members validated the descriptions and analyses of the case studies and their findings, addressed the potential for an incomplete range of sources having been gathered, overcame the risk of language differences adversely impacting, and prevented the possibility of inadvertent bias on the part of the researcher being injected into the work.
Finally, with regards to further research, this study has created several opportunities for future scholarly exploration and knowledge building concerning inter-organisational relationships between intelligence and law enforcement communities and agencies. For example, how effective have the approaches taken in Denmark, Finland, and New Zealand been in responding to transnational criminality? How have the governments and organisations involved addressed the issues of measuring success (or failure), resource allocation—particularly cross-sector funding, and provision of incentives to those involved to deliver the outcomes sought? And, how is accountability and oversight being managed when intelligence and law enforcement join-up to work on taskforces and multi-disciplinary teams? In the contemporary security environment with the complex security challenges it faces, the study of inter-organisational relationships between intelligence and law enforcement agencies remains, it is argued, topical and useful in understanding what is occurring in the relationship realm, and by informing those involved at the policy and practice levels of what options they have when it comes to working more effectively together.

- o O o -
References


Danish Security and Intelligence Service. (n.d. (a)). Center for Terror Analysis (CTA) Retrieved 01 April, 2014, from https://www.pet.dk/English/About%20PET.aspx

Danish Security and Intelligence Service. (n.d. (b)). About PET. Retrieved 1 April, 2014, from https://www.pet.dk/English/About%20PET.aspx

Danish Security and Intelligence Service. (n.d. (c)). PETs finances. Retrieved 1 April, 2014, from https://www.pet.dk/English/About%20PET.aspx


137


Supreme Administrative Court, the military intelligence establishment does not need to provide even more general information. (2007, 9 April 2007). *Yle*. Retrieved from http://yle.fi/uutiset/kho_armeijan_tiedustelulaitoksesta_ei_tarvitse_antaa_edes_yleisl uonteisia_tietoja/5781525


Appendix C

The following are examples of extracts from source documents showing how they were analysed during the research to determine which inter-organisational relationship type (or types) they were referring too. Examples from each case study are provided. For the Denmark and Finland case studies the examples also include extracts in the original Danish or Finnish, its translation using Google Translate, and how the text was then analysed.

Each example contains, in respect of the relationship type, a notation of either ‘(Direct)’ or ‘(Interpreted)’. The use of those terms is explained at page 37 in the body of the document.

NEW ZEALAND CASE STUDY

Government Expectations

Extract: “Under the new arrangement a specialised sub-committee of ODESC, known as the Intelligence Governance Committee, has been established. Cabinet directed that this committee should oversee governance and assurance in the intelligence community. It comprises the Chief Executives of three central agencies plus two others representing the interests of key customers of the intelligence community.”

Analysis:
Relationship type: Coordination (Interpreted) (See App. B: Coordination mind map features: formal design, control/regulating of work, agency ‘turf’ not given up, collective action);
Structure: Networked (more than two agencies involved);
Community: Intelligence Community focus;
Motivation: Encouraged (Cabinet direction, not legislated, and not voluntary engagement by the parties); and
Extent of engagement: Strategic (governance focus).

Intelligence Community

Extract: “A new relationship was established with the NZ Customs Service’s (NZCS) Integrated Targeting and Operations Centre (ITOC) in Auckland and the foundations were laid for the secondment of a NZSIS liaison officer from 1 July 2011.”

Analysis:
Relationship type: Collaboration (Interpreted) (See App. B: Collaboration features: [note: earlier review of ITOC confirmed it as a co-located, multi-agency entity where a diverse group of agencies worked together on border management/operational issues] intensive engagement (working in co-located environment), greater time commitment (co-locating directly with other agencies – staff member full committed to arrangement), shared risk and reward (co-located
multi-agency engagement), communication channels (co-location and multi-agency requires effective communication to help manage the interactions with other parties on a daily basis));

**Structure**: Networked (more than two agencies involved);

**Community**: Intelligence Community and Law Enforcement Community;

**Motivation**: legislation permits such engagement; and

**Extent of engagement**: Specific (border management / operational focus).

---

**Law Enforcement Community**


**Extract**: “Customs has established effective working relationships with other customs administrations and law enforcement agencies in New Zealand and overseas. These efforts, combined with technology advances and post-border investigative activity, have resulted in the exchange of valuable intelligence and joint operations to detect, disrupt and deter trans-national crime syndicates seeking to import illicit drugs and other threats to the New Zealand community. The establishment of the Integrated Targeting and Operations Centre (ITOC) and the National Maritime Coordination Centre [NMCC] are examples of Customs using its relationships with other agencies to improve its capability to protect the community by enhancing its access to intelligence and the capabilities of intelligence, defence, law enforcement, immigration and bio-security agencies together with Customs to more effectively deal with threats at the border.”

**Analysis**:

**Relationship type**: Coordination (Interpreted) (See App. B: Coordination features: controlling/regulating work (ITOC and NMCC able to coordinate action concerning border management and operation, and allocation of maritime assets to address multi-agency requirements; collective action (multi-agency environments established to achieve shared objectives/goals), Collaboration (Interpreted) (App. B: Collaboration features: Intensive relationships (joint operations and two co-located, multi-agency entities established), shared risk and reward (joint operations, multi-agency entities established), Shared objectives and goals (co-located entities, multi-agency engagement, focus on crime syndicates and drugs), communication channels (effective channels required to manage joint operations and multi-agency entities on a day by day basis));

**Structure**: Networked (multiple agencies involved);

**Community**: Intelligence Community and Law Enforcement Community;

**Motivation**: Voluntary (ITOC and NMCC not legislated for and initiated by Customs to better coordinate/collaborate in key areas); and

**Extent of engagement**: Specific (targeting of work, border management / operations, and maritime surveillance).
DENMARK CASE STUDY

Government Expectations
Source: DK106: Danish Prime Minister’s opening address to the Folketing (In English), 2011.

Extract: “In general, we will enhance Denmark’s involvement in the EU. I am certain that we will get more out of cooperating with our neighbours on, for example, cross-border crime than by building new inspection facilities at the Danish border. The Government also wishes to abolish the Danish opt-outs: the opt-out on defence and the opt-out on Justice and Home Affairs. The opt-out on defence prevents Denmark from participating in the important contributions made by the EU to promote peace and security in the world’s hotspots. The Government will therefore strive to abolish the opt-out on defence through a referendum. The opt-out on Justice and Home Affairs prevents Denmark from participating in EU cooperation in the fight against organised crime, terrorism, child pornography and human trafficking. This is about protecting our society. And about protecting the weakest in our society against gross exploitation. Denmark must assume responsibility in this area together with the rest of Europe.”

Analysis:

Relationship type: Cooperation (Direct) (See App. B: Cooperation features: low intensity and risk, achieve what cannot be achieved alone, formal pathway);
Structure: Networked (Demark and the EU / neighbours);
Community: Other (not defined, therefore, not coded);
Motivation: Encouraged (by the PM, Governments intentions, therefore, not legislated); and
Extent of engagement: Strategic (EU engagement, shared goals and objectives).

Intelligence Community
Source: DK024: FE's redegørelse for gennemførelse af benchmarkrapportens anbefalinger (In Danish), 2010 (FE Benchmarking update report from oversight committee, 2010).

Extract (Danish): “Anbefaling 10: FE bør styrke sit bidrag til indsatsen mod terrorisme (CT) ved at lade fem medarbejdere tilgå det nye center for terroranalyse, ved yderligere rekruttering for at modvirke huller i den tilbageværende CT-funktion, ved at videreudvikle og fokusere sin tekniske og HUMINT-kapacitet og ved at tilstræbe mere integreret samarbejde med PET om specifikke projekter.

Status
Anbefalingen er implementeret. FE har siden den 1. januar 2007 fast indstationeret 5 medarbejdere i Center for Terroranalyse (CTA). Etableringen af CTA ændrer ikke ved FE's ansvar i relation til terroranalyse, og udstationerede medarbejderes stillinger i FE er derfor blevet genbesat. FE's terrorbearbejdning er i 2008 blevet styrket ved ansættelse af yderligere analytikere samt en ændret organisering af terrorbearbejdningen.
Med det formål at fremme et tæt operativt samarbejde mellem de to tjenester samt at forbedre støtten til PET og CTA har FE en medarbejder stationeret i PET's operative afdeling. Udvekslingen af personale drøftes i øvrigt løbende på de regelmæssige møder, der afholdes mellem PET's ledelse og FE's ledelse.

Der er i relevant omfang et tæt samarbejde mellem FE's terroranalytikere og PET's efterforskningsskaber, ligesom FE fremsender samtlige efterretningsvurderinger med et terrorrelateret indhold til PET og CTA. Desuden videregiver FE løbende oplysninger til PET, som er medtaget i tjenestens virksomhed, om danske statsborgere og personer, der opholder sig i Danmark.

Extract (translated into English using Google Translate): “Recommendation 10:

FE should strengthen its contribution to the fight against terrorism (CT) by leaving five people accessing the new center for terrorism analysis by further recruitment to offset gaps in the remaining CT function, by further developing and focus its technical and HUMINT capabilities and by seeking more integrated cooperation with PET on specific projects.

Status

The recommendation has been implemented. FE has since 1 January 2007, the relocated 5 staff at the Center for Terror Analysis (CTA). The establishment of the CTA does not change the FE's responsibilities in relation to terrorism analysis and expatriate staff positions in FE has therefore been filled. FE terrorist working in 2008 was strengthened by hiring additional analysts and a change in the organization of terrorbearbejdningen.

In order to promote close operational cooperation between the two services and to improve support for PET and CTA has FE a team stationed in PET's operational department. The exchange of staff discussed also ongoing at the regular meetings held between PET's management and FE's management.

It is appropriate, close cooperation between FE terrorist analysts and PET exploration groups, like FE shall forward all intelligence assessments with a terrorism-related content for PET and CTA. Furthermore pass FE current information to PET, which is included in the service business of Danish nationals and persons residing in Denmark.”

Analysis:

Relationship type: Cooperation (Interpreted) (See App. B: Cooperation features: sharing of information (intelligence assessments on terrorism shared)), Collaboration (Interpreted) (App. B: Collaboration features: shared risk and reward (co-location of personnel in CTA multi-agency unit), intensive engagement (stationing of team within another agency’s operational unit), greater time commitment (management meetings, staff sharing, commitment to CTA of 5 staff who are no longer working only for FE));

Structure: Dyadic (PET/FE);

Community: Intelligence Community;

Motivation: Legislation and encouraged (legislation permits FE/PET relationship, benchmarking report encourages greater engagement); and

Extent of engagement: Specific (terrorism focus).
Law Enforcement Community


Extract (translated into English using Google Translate): “National Police responsible for the overall coordination of the police's overall efforts in this area and as part of this, receive, collect, compare, process and disseminate the National Police relevant information from the national police to assist the police districts to prevent and solve crime of circle cross-border and organized nature (so-called analysis and monitoring). The information provided by the National Police receive from police districts, supplemented in the case of information from national and international partners. The National Police shall, on the basis ongoing analyzes of the situation at the national level and communicate the overall picture in the area for police districts in order to ensure effective and targeted planning of police overall efforts in the area - this could be a designation of concrete targets for exploration or reduction by a task force with personnel from the National Police and the relevant police. National Police can be based on all the collected and processed information identifying groups or individuals related to the biker and gangs who have completed or are presumed would implement crime. In this way provides the basis for concrete investigations.”

Analysis:

Relationship type: Cooperation (Direct) (See App. B: Cooperation features: information sharing, working with others to achieve what cannot be achieved alone), Coordination (Direct) (App. B: Coordination features: work regulation/control (overall coordination; completing analysis and disseminating information to designate targets for exploration), collective action (multi-organisational task force activity));

Structure: not defined (involves police and ‘partners’ but numbers involved not clear, could be dyadic or networked, therefore not coded);

Community: Law Enforcement Community and ‘others’ (‘others’ not defined, may include Intelligence Community (IC), but may not, therefore not coded as including IC);
Motivation: Legislated (police function to address crime), Encouraged (police leading efforts of themselves and others through their own initiative);

Extent of engagement: Specific (focus on bikers and gang crime, cross-border and organised).

FINLAND CASE STUDY

Government Expectations

Extract: “… Intelligence, analysis and intersectoral co-operation, in particular in the EU and at the international level, are developed. The exchange of information is increased on combating, exposing and solving cross-border crime as well as on operations within the EU and with countries highly significant for Finland. This makes it easier to combat various threats through intelligence-based law enforcement. … By engaging in nation-wide security planning, it is possible to have the various actors in society committed as partners in the fight against crime. Measures related to the surveillance of organised crime, financial crime and foreign workers are developed. … Co-operation between the law enforcement authorities, i.e. the Police, Finnish Customs and the Border Guard (PCB authorities) is intensified and focuses on crime-fighting. The expansion of the Schengen area presupposes even more effective and comprehensive crime-fighting on the national level, between old Member States and also among the law enforcement authorities of the new Member States. Operational inter-authority co-operation is developed in line with the principles of Finnish PCB co-operation. … Adopted in the Government Resolution in 2010, the recommended measures presented in the national counter-terrorism strategy will be implemented. To combat terrorism, a terrorism situation picture is created. This includes data on terrorist activities threatening Finland, possible targets of terrorism as well as persons deemed to be a threat and who either reside in Finland or threaten Finland. As the situation picture is compiled, reports from institutions participating in the EU’s police and judicial authorities’ co-operation as well as other international contacts are utilised. …”

Analysis:

Relationship type: Cooperation (Direct) (See App. B: Cooperation features: less intensive and lower risk, information sharing), Collaboration (Interpreted) [note: mention of ‘partners’ and ‘intensified cooperation’ based on PCB Cooperation Act which was assessed to empower not just cooperation, but also coordination and collaboration, mention of operational inter-authority cooperation] (App. B: Collaboration features: intensive engagement, greater time commitment, achieve what cannot be achieved alone, formal pathway, shared objectives and goals (national counter-terrorism strategy));

Structure: Networked (multiple agencies);

Community: Law Enforcement Community and others;

Motivation: Legislation (PCB Cooperation Act mentioned); and

Extent of engagement: Specific (operational engagement on particular security issues as listed in extract).
Intelligence Community

Extract: “In accordance with its basic task, the Police is [sic] in charge of counterterrorism in Finland. Within the Police, Supo is the authority in charge of national and international cooperation among authorities.”

Analysis:

Relationship type: Cooperation (Direct) [note: assessed use of the word in context] (App. B: Cooperation features: Achieve what cannot be achieved alone)

Structure: not fully defined, therefore, not coded

Community: Intelligence and Law Enforcement (Police and Supo both mentioned)

Motivation: Legislation (‘basic task’ reference to police tasks determined by legislation)

Extent of engagement: Specific (counterterrorism focus)

Law Enforcement Community


Toteutettuja toimenpiteitä - esimerkkejä


Järjestäytyneen rikollisuuden torjunta.”

Extract (translated into English using Google Translate): “Prevention of and fight against organised crime, the conditions have been developed. Organized crime, the challenges have increased. As a new and growing phenomenon of the so-called. performances in hit and run
[note: hit and run was a term encountered elsewhere in the research and related to cross-border crime from predominantly Baltic State citizens who entered Finland, committed theft or burglary type crimes, and then fled back to their home country], which have increased significantly. Threat of organized crime specifically targets certain sectors, which has also been targeted prevention activities in collaboration with business and industry. The measures taken – examples: Fight against organized crime conditions to ensure. The authorities in combating organized crime operating conditions have improved. PTR (police, customs, border) cooperation in the Act and Decree entered into force on 1.1.2010. In more detail, the PTR authorities, for the co-operation agreed upon co-operation arrangements. PTR –rikostiedustelua and analysis function in the organization and management has been modified to include the police administration structural reforms. Police target pesticides order is renewed cooperation between various units underscored by the emphasis on, and target prevention regulations related to financing the process of being reorganized to better meet the real-time performance requirements. The preliminary investigation authorities have been involved in a number of international investigative teams and yhdysmiesverkostoa has been extended. Cooperation has been intensified the enforcement of sentences with the authorities in order to prisons recruitment of organized crime groups to prevent. Subject matter relating to the prevention of financial process has been revised and entered into force on 1.1.2011. The reform will deliver real-time financial assistance for projects.”

Analysis:

Relationship type: Cooperation (Direct) [note: use of the word in context with reference to the PTR Cooperation Act. Also mention in the extract of ‘collaboration with business and industry,’ but no mention regarding governmental inter-agency engagement being involved, therefore, collaboration not coded];

Structure: Networked (police, customs and border guards);

Community: Law Enforcement;

Motivation: Legislation (Act and decree mentioned); and

Extent of engagement: Strategic (mention of the Cooperation Act entering into force which creates shared objectives and goals) and Specific (risk analysis, focus on organised crime groups).

Finally, an example is provided of an occasion where, due to the shared features identified between the NC3 relationship types (refer to Table 2.4 at p. 19), it was not possible to code the relationship text to a particular relationship type.


Extract: “Traditionally most intelligence agencies have operated relatively independently of each other and have not been well-aligned with broader national security objectives. Work is underway to change this so that intelligence agencies have even closer relationships with, for example, law enforcement agencies such as Police, Customs and the Immigration Service.”
Analysis:

*Relationship type:* Not defined and no NC\textsubscript{3} descriptors used. ‘… even closer relationships …’ could refer to cooperation, coordination and/or collaboration, therefore, this extract not coded for relationship type;

*Structure:* Networked (mention of intelligence agencies and various Law Enforcement Community agencies);

*Community:* Intelligence and Law Enforcement;

*Motivation:* Encouraged, no mention of legislation being enacted or changed; and

*Extent of engagement:* Strategic (national security).
1 April 2014

Mr Richard Shortt
32 Leane Street
Hughes
Canberra
ACT 2605

Dear Mr Shortt,

The AGSP HREC Committee has approved your proposal “Intelligence meets Law Enforcement: Heartache or Harmony in responding to wicked issues such as transnational criminality” for a twelve month period from 1 April 2014.

The protocol number issued with respect to this project is 110-2014-11. Please be sure to quote this number when responding to any request made by the Committee.

You must notify the Committee immediately should your research differ in any way from that proposed.

You are also required to complete a Progress Report form, which can be downloaded from http://www.csu.edu.au/research/ethics_safety/human/ehrc_managing and return it on completion of your research project or by your next progress report if your research has not been completed by that date.

The Committee wishes you well in your research and please do not hesitate to contact Dr Hugh McDermott on telephone (02) 9932 5206 or email hmcdermott@csu.edu.au if you have any enquires.

Yours sincerely,

Hugh McDermott
Presiding Officer
AGSPS HREC Committee
Direct Telephone: (02) 9932 5206
Email: hmcdermott@csu.edu.au
Co: Dr. Hank Prunckun
Dear [name and title of potential expert panel member]

I refer you to our recent [telephone call, meeting, or email correspondence] regarding my PhD research and thank you for indicating your willingness to consider being an expert panel member for my case study of XXX.

This letter contains further information on the research, the expert panel member process and the indicative timeline concerning your involvement.

To summarise my research, its aim is to determine what inter-organisational relationships have developed between the intelligence and law enforcement communities in mid-sized countries in an effort to address the wicked issue of transnational criminality, and can study of these lead to policy benchmarks for similar sized nations to consider. The research will include case studies of three mid-sized countries: New Zealand, Denmark and Finland.

For each case study my methodology calls for an expert panel member from each country. All three expert panel members will have professional backgrounds that ensure they are able to provide informed comment on the material provided. The experts also agree to have their name and relevant employment background acknowledged when the dissertation is published for the role they have performed.

The role of the expert panel member is to determine if the research has correctly identified the core elements of their nation’s approach and whether any important element (or elements) has been overlooked, overstated, or misinterpreted. The panel member’s opinions will increase the rigour to the final findings, manage any bias that may have occurred, and steer any additional research required to overcome identified gaps.

The review process will follow the steps set out below:

- The relevant case study is completed to first draft stage;
- It will be emailed to you for review;
- Your review the draft case study will be with aim of answering the following three questions:
  1. In your opinion, has the research capture the essence of the inter-organisational relationships between the intelligence and law enforcement communities in the researched nation, concerning the issue of transnational criminality?
  2. If it is your view that there is a gap (or gaps) in the research and/or its findings, briefly outline what is the gap (or gaps) is?
  3. What existing secondary source documents, that are publicly available, would help me address the identified gap (or gaps), and where may these be found?
- You then email your answers to the three questions back to me, and I will address—by way of additional research—any matters raised under Questions 2 and 3;
- When I have completed any additional research, the second draft of the case study will be emailed to you for review, with the aim of answering the following question:
1. In your opinion, has the additional research resulted in the issue(s)—raised during your first review—being satisfactorily addressed, and if not, why not?

- You will then email your response back to me;
- If your answer is that they have not, then I will enter discussions with my PhD supervisor for advice and guidance on how I should proceed from that point on. You will be advised of the result of these discussions; or
- If your answer is that they have, then the case study will progress to final draft status in preparation for publication of the dissertation.

The research timeline identifies that the case study of XX will be commenced in MM of YY. It is anticipated the first draft will be provided to you for review in MM of YY. A response within 60 days would be appreciated to help keep the research process moving towards its completion date. The second review, should any additional research be required, will occur when the research is completed according to timeline for that work which I will provide you within two weeks of receiving of your initial reply. Once the second draft has been forwarded to you for review, a response would again be appreciated within 60 days of receipt.

Please view these timeframes as indicative. I appreciate that your time is limited and that other factors may impact your ability to respond as suggested.

If, after reading this description of the expert panel concept, you are agreeable to participating as a panel member, please confirm by email, and include any questions you may have. Alternatively, if you decide to opt out of the process described and to not be a panel member, please also communicate this decision to me by way of email. If you choose to opt out, but know of a colleague who is suitable for the role, please advise me of this in your reply.

Whatever the decision you make, thank you again for considering taking on this role, and I look forward to hearing from you.

Yours sincerely

Richard Shortt
PhD CANDIDATE
<table>
<thead>
<tr>
<th>Case study</th>
<th>Expert panel member</th>
<th>Indicative feedback</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Zealand</td>
<td>Mr R Mark Evans Deputy Chief Executive New Zealand Police</td>
<td>1) The Policing Act also defines ‘National Security’ as one of the functions of Police – I would argue this provides an equally valid mandate.</td>
<td>1) Review the wording of the paragraph and incorporate this matter, after confirmation through review of the Policing Act source. RS 29 Aug 2014 Agreed. Paragraph updated as suggested by expert reviewer. RS 29 Aug 2014</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2) An exaggeration of the influence and importance of the role. In practice the IC did not co-ordinate all NZ intelligence work (indeed he did not even coordinate all the intelligence work within the NZIC) and it is arguable that much of what was coordinated was not in fact ‘intelligence’ (rather the supporting, logistical and financial arrangements necessary for it to function effectively). The position had no decision rights over any non-NZIC agency. That said, the position did have a mandate to improve collaboration and supported a whole of government agenda. One might legitimately ask though – given the size of the NZSIS and the major investment in ‘IC Community House’ (Pipitea) for which government expected to see a return – what is the realistic alternative…?</td>
<td>2) Review the paragraph and its contention. Can Evans’ view be incorporated? Or, does it belong elsewhere in regards to the NZCS? RS 29 Aug 2014 Paragraph text reviewed along with sources relevant to topic. Agree with point made by Evans. Paragraph wording adjusted to reflect the feedback comment from Evans. RS 29 Aug 2014</td>
</tr>
<tr>
<td>Denmark</td>
<td>Ms Kira Rønn PhD Strategic Analyst National Danish National Police</td>
<td>1) …a challenge here is the language. “Samarbejde” in Danish will (you point to this fact yourself) most often be applied when any type of inter-organisational relationship is presented. The particular way of collaborating (“samarbejdsrelation”, “samarbejdsforhold”) i.e. via networks, partnerships etc. could specify the distinctions you attempt to identify in the study. However, such distinctions will (in my view) most often not be specified when communication about the ways of cooperating.</td>
<td>1) Agreed. Language is a challenge in the Danish context for the reasons outlined by Rønn. When classifying the data, and being aware of the issue related to language use, context was looked for to help make the determination as to which option to use. Example: If a relationship involved use of a joint-taskforce/investigation then such work would be classified as collaboration as both parties were</td>
</tr>
</tbody>
</table>


could imagine that this fact might lead to difficulties when classifying the material in terms of types of relationships. A central methodological question here would be: Could the most common types of relationship identified in the Danish case just as well be “collaboration” due to the language barrier? Would it be an idea to specify this – maybe when discussing the results of the case study?

working together and had given up organisational turf to do so – a factor associated with collaboration. Furthermore, multi-disciplinary teams (joint taskforce) are another feature of collaboration, but not of simple cooperation.

**Action:** Review the methodology to confirm that the focus on context was increasingly important in the Danish case study given the language issue, and does the explanation clarify how efforts were made to render the data credible/accurate.

27 Jan 2015: Review of methodology to determine if this issue has been addressed satisfactorily?

The text below, taken from the Danish case study methodology section, addresses the issue raised. It has been added too (see highlighted segment) to better clarify the approach taken to gathering the data for this research:

“The above discovery, coupled with the earlier identified issue of the Danes using one word for inter-organisational relationships, meant the researcher’s interpretation of the type of inter-organisational relationship being written about, and described by the words samarbejde in Danish language sources, and cooperation or collaboration in English language sources, was particularly important and central to the case study. The availability of the earlier created mind maps for the NC3 relationship types and the analysis of the distinct features for each relationship type discussed in the source documents enabled those interpretations to be completed with confidence.”
Therefore, as was done in the New Zealand case study, when text about an inter-organisational relationship associated with transnational criminality was encountered, the type of relationship was classified as either a direct or interpreted item of data through consideration of both the descriptive words used and the context surrounding the use. For example, a direct classification signified that the word used to describe the relationship type aligned with the mind map features for that relationship type, (e.g. use of the word samarbejde in a Danish language source, or cooperation in a Danish source that had been translated into the English language), thus indicating a correct use of the word. Alternatively, an interpreted classification signified that a word used to describe a relationship type did not align to the relationship type indicated, and that an alternative relationship type had actually being described (e.g. use of the word samarbejde or cooperation actually aligned with the features of a coordination or collaboration relationship type). Furthermore, if an inter-organisational relationship was described without the use of an NC3 descriptor word, it was also recorded as an interpreted classification for the NC3 relationship type it most closely aligned too.

Through the above described process, most Danish language and English language data could be confirmed as pertaining to one particular inter-organisational relationship type, while some could only be narrowed to two or three of the four NC3 types. The inability to narrow all of the data to one
relationship type was due to the shared features some relationship types enjoyed, as discussed earlier in Chapter 4 (see Table 2.4). If a relationship type could not be narrowed to one particular type through review of the context and NC3 mind maps, it was not recorded in the data. This non-recording avoided the danger of double counting any individual relationship mentions in the data (i.e. counting a mention as both a coordination and collaboration). This had the unfortunate affect of reducing the amount of data available for analysis; however, it strengthened the validity of the data gathered.

In the case of both direct and interpreted classifications, each time a relationship type was confirmed in a source document it was assigned the value ‘1’. The values were subsequently totalled for each source and recorded in the Denmark case study spreadsheet in either the direct or interpreted data columns alongside the title of the source being reviewed. At the same time, using the context surrounding the relationship mentions, qualitative data was also recorded. That data concerned the structure involved with the relationship (dyadic or networked) and the identity of the communities (or community) involved (i.e. IC and/or LEC, or others), the motivation for the relationship and the extent of the relationship. The data record was completed with a short commentary summarising the source and its relevance to the study.”

I believe this text suitably addresses the issue raised by the expert reviewer.
1) In response to first question asked: Based on my experience, I do believe that the research has captured the essence of the inter-organizational relationships between the intelligence and law enforcement communities in Finland. Finland has strong and independent intelligence and law enforcement agencies and these agencies often interact through cooperative arrangements.

2) For example, Figures 4.26, 4.27 and 4.28, show that the government expectations seem to be matched pretty well by the law enforcement community, whereas the same does not seem to apply to the intelligence service. Similarly, there seemed to be some disparities in the case

The above response was provided to Dr Rønn along with all of the responses to the points she raised. In February 2015 Dr Rønn replied thanking the researcher for “the thorough responses to my comment [sic]. I have no further questions.”

Finland

Mr Stefan Aniszewski
Senior Technical Officer
Former Finnish government official and employee of Finnish Customs

2) You write on p. 1 that you could not find any sources from the Danish Defense Intelligence Service regarding the inter-organisational relationship. I have briefly looked on their website, and they write about their “samarbejde” cooperation on these pages:

http://fe-ddis.dk/Opgaver/Samarbejde/Pages/Samarbejde.aspx

http://fe-ddis.dk/Opgaver/Samarbejde/Akademisk-samarbejde/Pages/Akademisk-samarbejde.aspx

2) Noted.

Action: Review the two links provided. It may be that this information is already held on file, however, if not gather and assess relevance to the research.

21 Jan 2015 – first website page had been gathered and assessed. Was outside the study timeframe, but did discuss PET and CTA close cooperation.

Second website page had not been previously gathered. Page reviewed and while it discussed collaboration with academics, its content was determined to be not relevant to the research.

2) Noted. The points raised by the reviewer will be discussed in the Discussion chapter of the study, which will bring together the case studies to consider what the findings from them are. RS 27 Apr 2015
of engagement occurrences when comparing the expectation and the actual delivery by the communities (Figures 4.32, 4.33, and 4.34). What do these disparities mean and what is their effect to the final results of the study…