

**‘A critical assessment of international legislative measures
towards combating terrorist financing over the internet with
primary focus on appropriateness and effectiveness’**

Georgina Webb

**LL.B
LLM**

**A thesis submitted in partial fulfilment of the requirements of
the University of the West of England, Bristol
for the degree of Doctor of Philosophy**

**Faculty of Business and Law
University of the West of England, Bristol**

April 2018

Contents

Abstract	pp1-2
Chapter one: Introduction	p3-35
1.1. The Evolution of Terrorism	pp3-5
1.2. Financial Crime and the issue of terrorist financing	pp5-8
1.3. The use of the Internet by terrorists	pp8-10
1.4. Structure of the Thesis	pp10-26
1.4.1. The definition of effectiveness	pp12-18
1.4.1.1. Effectiveness in the context of counter-terrorist financing	pp12-16
1.4.1.2. Effectiveness in the context of Internet transactions	pp16-18
1.4.2. The definition of appropriateness	pp18-26
1.4.2.1. Appropriateness in the context of counter-terrorist financing	pp20-23
1.4.2.2. Appropriateness in the context of Internet transactions	pp23-26
1.5. Structure of each chapter	pp26-35
1.5.1. Chapter Three: Background to the international position on financial crime and regulation of the Internet before 9/11	pp26-27
1.5.2. Chapter Four: The United States	pp27-29
1.5.3. Chapter Five: The United Kingdom	pp29-31
1.5.4. Chapter Six: Kingdom of Saudi Arabia	pp31-33
1.5.5. Chapter Seven: The United Nations and International Organisations/ Conclusion	pp33-35
Chapter two: Methodology & Literature Review	pp36-61
2.1. Introduction	pp36-38
2.2. Rationale of using Doctrinal Methodology	pp38-40
2.3. Rationale of using Qualitative and Comparative Research Design methods	pp40-43
2.4. General Research Questions	pp43-46
2.5. The selection of key examples	pp46-54

2.5.1. The United States	pp47-51
2.5.2. The United Kingdom	pp51-53
2.5.3. Kingdom of Saudi Arabia	pp53-54
2.6. Literature Review	pp54-61
2.6.1. Counter-Terrorist Financing after 9/11	pp55-57
2.6.2. Internet filtration and surveillance in the modern age	pp57-59
2.6.3. Overall Data Collection Techniques	pp59-60
2.7. Conclusion	pp60-61

Chapter three: Background to the international position on financial crime and regulation of the Internet before 9/11

3.1. Introduction	pp62-63
3.2. Money Laundering	pp63-101
3.2.1. The United Nations and other International Organisations	pp67-80
3.2.1.1. The move towards counter-terrorist financing	pp77-80
3.2.2. The United States	pp80-91
3.2.2.1. The move towards counter-terrorist financing	pp85-91
3.2.3. The United Kingdom	pp91-95
3.2.3.1. The move towards counter-terrorist financing	pp93-95
3.2.4. The Kingdom of Saudi Arabia	pp96-101
3.2.4.1. The move towards counter-terrorist financing	pp97-101
3.3. Technology	pp102-131
3.3.1. The United Nations and other International Organisations	pp105-113
3.3.1.1. Direct solicitation of donations	pp105-107
3.3.1.2. Use of legitimate sources	pp107-108
3.3.1.3. Cybercrime	pp108-113
3.3.2. The United States	pp113-119

3.3.2.1. Direct solicitation of donations	pp114-116
3.3.2.2. Use of legitimate sources	pp116-117
3.3.2.3. Cybercrime	pp117-119
3.3.3. The United Kingdom	pp119-127
3.3.3.1. Direct solicitation of donations	pp119-122
3.3.3.2. Use of legitimate sources	pp122-123
3.3.3.3. Cybercrime	pp123-127
3.3.4. The Kingdom of Saudi Arabia	pp128-131
3.3.4.1. Direct solicitation of donations	pp129-130
3.3.4.2. Use of legitimate sources & Cybercrime	p131
3.4. Conclusion	pp131-134

Chapter four: The United States **pp135-201**

4.1. Introduction	pp135-139
4.2. Direct solicitation of donations	pp139-167
4.2.1. Websites	pp140-150
4.2.2. Electronic Communications	pp150-167
4.3. Legitimate sources of finance	pp167-186
4.3.1. Charities	pp168-175
4.3.2. Financial Institutions	pp175-186
4.4. Cybercrime	pp186-199
4.4.1 Cyberlaundering	pp187-197
4.4.2. Online Fraud	pp197-199
4.5. Conclusion	pp200-201

Chapter five: The United Kingdom **pp202-309**

5.1.	Introduction	pp202-205
5.2.	Direct solicitation of donations	pp206-264
5.2.1.	Websites	pp207-225
5.2.2.	Electronic Communications	pp225-263
5.2.2.a.	Content of electronic communications	pp226-240
5.2.2.b.	Non-content of electronic communications	pp240-247
5.2.3.	The Investigatory Powers Act	pp247-264
5.2.3.a.	The Investigatory Powers Act vs the CJEU	pp260-262
5.2.3.b.	The Investigatory Powers Act vs Data Protection Directive 2016	pp262-264
5.3.	Legitimate sources of finance	pp264-295
5.3.1.	Charities	pp265-280
5.3.2.	Financial Institutions	pp280-295
5.4.	Cybercrime	pp295-307
4.4.1	Cyberlaundering	pp296-302
4.4.2.	Online Fraud	pp302-307
5.5.	Conclusion	pp307-309

Chapter six: The Kingdom of Saudi Arabia **pp310-347**

6.1.	Introduction	pp310-312
6.2.	Direct solicitation of donations	pp312-328
6.2.1.	Websites	pp313-322
6.2.2.	Electronic Communications	pp322-328
6.3.	Legitimate sources of finance	pp328-342
6.3.1.	Charities	pp328-333
6.3.2.	Financial Institutions	pp333-342

6.4.	Cybercrime	pp342-345
6.5.	Conclusion	pp345-347

Chapter seven: The United Nations and International Organisations – Conclusion

pp348-414

7.1.	Introduction	pp348-350
7.2.	Direct solicitation of donations	pp350-364
7.2.1.	Websites	pp351-355
7.2.2.	Electronic Communications	pp355-364
7.3.	Legitimate sources of finance	pp364-371
7.3.1.	Charities	pp364-366
7.3.2.	Financial Institutions	pp366-371
7.4.	Cybercrime	pp371-375
7.5.	Conclusion	pp375-414
7.5.1.	The effectiveness of international efforts to combat terrorist financing via the Internet	pp375-384
7.5.2.	The appropriateness of international efforts to combat terrorist financing via the Internet	pp384-394
7.5.2.1.	The United States	pp386-387
7.5.2.2.	The United Kingdom	pp388-390
7.5.2.3.	The Kingdom of Saudi Arabia	pp390-392
7.5.2.4.	The United Nations and International Organisations	pp392-394
7.5.3.	Suggestions for reform	pp394-414
7.5.3.1.	Improvements to domestic law	pp394-404
7.5.3.1.a.	The United States: Separating anti-money laundering from counter-terrorist financing	pp396-397
7.5.3.1.b.	The United Kingdom: using intercept evidence in court	pp397-398
7.5.3.1.c.	The United Kingdom: Balancing surveillance with privacy	pp398-401

7.5.3.1.d. The United Kingdom: Using innovation to capture acts of cheap terrorism	pp402-403
7.5.3.1.e. Kingdom of Saudi Arabia: Specific Cybercrime laws	p404
7.5.3.2. Improvements to international law	pp405-414
7.5.3.2.a. A definition of terrorism	pp406-408
7.5.3.2.b. A re-evaluation of the Suspicious Activity Report system	pp408-409
7.5.3.2.c. Internet Governance	pp409-410
7.5.3.2.d. Adoption of the European Cybercrime Convention 2001 through a Security Council Resolution	pp410-414
List of abbreviations	pp415-418
Bibliography	pp419-502