The relationship between legal systems and legal responses: the case of cyberterrorism in China and England & Wales

Xingxing Wei
Submitted in accordance with the requirements for the degree of Doctor of Philosophy (PhD)

School of Law and Politics
Cardiff University
September 2021
Acknowledgements

The doctoral research process is a long and challenging process. During this process, I have suffered a lot, and also received a lot of assistance and encouragement. Therefore, I would like to extend my sincerest thanks and best wishes to those who helped and supported me. First of all, I want to thank myself for my unremitting efforts and perseverance for supporting me in completing my PhD research. Studying abroad for PhD degree has always been my dream. When the dream shines into reality, it is due to my persistence and curiosity about the unknown. I have experienced countless ups and downs in recent years, but in the end I did it.

Secondly, I would like to express my deeply grateful to my two supervisors, Dr. Bharat Malkani and Dr. Adam Edwards, for their professional and patient supervision in writing this long piece of doctoral dissertation. They consistently encourage me to refine my analytical arguments, critical thinking, logical structure, etc. As an interdisciplinary research, it is my honor to have these two supervisors to provide analytical comments from law and criminology perspectives. Without their supervision, it impossible for me to complete this thesis.

Thirdly, I want to thank for the scholarship granted by the China Scholarship Council and Cardiff Law school. Without their financial support, I would not be able to complete my PhD research without financial burden. Meanwhile, I also want to thank Professor Wang Xiumei and Dr. Zhao Chenguang, who encouraged and assisted me to apply this PhD study, and also invited me to participate in the National Social Science Foundation's research on terrorism and extremism, which also provided strong data support for my doctoral research.

I warmly express my thanks to Abby, Sharron, Sarah and other staffs in Postgraduate study team, who gave me generous help and support. I also want to show my appreciate to Professor Jiang Wenguo, who helped me negotiate with the University and the Law school, and prompted me to adjust the direction of my thesis to make it go smoothly when my PhD career was at a standstill in my final year.
Lastly, I would like to extend my gratitude to my family and friends (Tian Yanan, Zhou Yi, Jing song, Xue Jingjing, Yang Likun, Zhang Qiang and other friends), especially under this risky and uncertain circumstance of COV-19. In particular when I was desperate, it was my parents who kept encouraging me, comforting me and giving me motivation to continue my PhD research. During my study in Cardiff, it is my honor to meet my church friend Denis, Freda and Ann and Brian, Lindsay. When I feel lonely and lost in my thesis study, they can always listen to my troubles and encourage me to give me some constructive comments. Ann always calls me to care about my current situation, especially when I am suffering from toothache, to provide me with professional advice and help.
# Contents

ACKNOWLEDGEMENTS ................................................................................................................................................. I

LIST OF LEGISLATION ........................................................................................................................................... VIII

ABBREVIATIONS ......................................................................................................................................................... X

FIGURES ...................................................................................................................................................................II

ABSTRACT ................................................................................................................................................................ III

CHAPTER 1 INTRODUCTION .................................................................................................................................. 1

1.1 RESEARCH BACKGROUND .................................................................................................................................. 1

1.2 RESEARCH OBJECTIVES AND QUESTIONS ...................................................................................................... 6

1.3 ORIGINALITY AND CONTRIBUTION .................................................................................................................. 7

1.4 RESEARCH JUSTIFICATIONS ................................................................................................................................ 12

1.5 OUTLINE OF CHAPTERS ..................................................................................................................................... 14

CHAPTER 2 LITERATURE REVIEW .................................................................................................................. 20

2.1 INTRODUCTION .................................................................................................................................................... 20

2.2 DEFINING “CYBERTERRORISM” ............................................................................................................................ 21

   2.2.1 Literature Review of Definitions of Cyberterrorism in China ................................................................. 27

   2.2.2 Literature Review of Definitions of Cyberterrorism in E&W ................................................................. 30

2.3 LITERATURE REVIEW OF THE RELATIONSHIP BETWEEN A LEGAL SYSTEM AND CYBERTERRORISM ...... 35

   2.3.1 The Relationship between a Legal System and the Legal Response .................................................... 35

   2.3.2 Regime Types and Effectiveness of Combating Cyberterrorism .......................................................... 37

2.4 LITERATURE REVIEW OF CRITICAL ANALYSES OF LEGAL RESPONSES TO CYBERTERRORISM ....... 39

2.5 CONCLUSION ........................................................................................................................................................ 52

CHAPTER 3 METHODOLOGY ........................................................................................................................ 53

3.1 INTRODUCTION .................................................................................................................................................... 53

3.2 DOCTRINAL METHODOLOGY ............................................................................................................................ 55

3.3 COMPARATIVE METHODOLOGY .......................................................................................................................... 56

   3.3.1 Cultural Comparative Methodology ......................................................................................................... 58

   3.3.2 Comparability ............................................................................................................................................. 59

   3.3.3 The Four Reasons Behind Using the Comparative Legal Method? ....................................................... 61
3.3.4 How is a Comparative Study Conducted? ........................................................................................................ 66
3.3.5 Limitations of Comparative Legal Methodology ........................................................................................ 68
3.4 Socio-legal Methodology ..................................................................................................................................... 68
3.5 Conclusion ........................................................................................................................................................... 72

CHAPTER 4 THE LEGAL SYSTEM IN CHINA ........................................................................................................ 74

4.1 Introduction .......................................................................................................................................................... 74
4.2 Rule by Law, Rule of Law and Rule of Man .................................................................................................... 75
   4.2.1 Defining the “Rule of Law” from Western and Chinese Perspectives ................................................... 75
   4.2.2 The Chinese Socialist “Rule of Law” or “Rule by Law” ....................................................................... 79
4.3 Distinctive Characteristics of the Legal System in China ........................................................................... 83
   4.3.1 Concentration of Powers ........................................................................................................................ 84
   4.3.2 Lack of Judicial Independence ............................................................................................................... 87
   4.3.3 Different Understanding of Human Rights Protection ......................................................................... 88
   4.3.4 Lack of Checks and Balances on Human Rights Protection ............................................................... 92
4.4 Basic Criminal Law Principles in China ..................................................................................................... 95
   4.4.1 The Principle of Proportionality .......................................................................................................... 96
   4.4.2 The Principle of Certainty of Law ......................................................................................................... 98
   4.4.3 The Principle of Legality (Nullum crimen sine lege, nulla poena sine lege) ........................................... 100
   4.4.4 The Principle of Minimal Criminalisation ......................................................................................... 101

CHAPTER 5 THE LEGAL RESPONSE TO CYBERTERROISM IN CHINA .................................................. 105

5.1 Introduction ....................................................................................................................................................... 105
5.2 Prevention and Pre-emptive Tendency ........................................................................................................ 107
5.3 National Security and Social Stability Priority over Human Rights Protection in the Anti-terrorism Laws and Enforcement ........................................................................................................... 112
5.4 Broad and Vague Definition of Terrorism ................................................................................................ 117
5.5 Criminalisation of a Wide Range of Terrorism Precursor Offences ......................................................... 125
   5.5.1 Intensification of the Crackdown on Association with or Membership of Proscribed Organisations ................................................................. 128
   5.5.2 Suppressing Financial Assistance or other Tangible Support for Terrorism ....................................... 129
   5.5.3 Criminalisation of Publishing of Statements Likely to be Understood as Direct or Indirect Encouragement or other Inducement to Commit, Prepare or Instigate Acts of Terrorism ...... 131
   5.5.4 Criminalisation of Terrorist Propaganda and Incitement (Art. 120c) .................................................. 132
5.5.5 Criminalisation of a Broad Scope of Preparatory Terrorist Acts (Art. 120b) ...................... 136
5.5.6 Overly Broad Offence of Collection of Information or Possession of Items for Terrorism Purposes .............................................................................................................................................................................. 138
5.6 Aggravated Punishment for Terrorism .................................................................................. 139
5.7 Vague and Uncertain Criteria of Measuring the Severity of "Circumstances" ...................... 145
5.8 Broad Discretion of Executive Organs to Designate Proscribed Terrorist Organisations .... 147
5.9 Enforcement of the Criminal Law and Counter Terrorism Law ........................................ 151
   5.9.1 The Expanding Power of Administrative Departments (mainly the police) during Counterterrorism Efforts (such as investigation and detention) ........................................................ 151
   5.9.2 Limited Safeguarding of Suspects' Rights in Terrorism-related Cases .......................... 153
   5.9.3 Empower Executive Organs with Broad Discretion to Issue Control Orders .............. 154
   5.9.4 Tendency of Using Non-criminal Disruption Methods to Deal with Precursor Terrorism-related Offences ...................................................................................................................................................... 156
5.10 Conclusion ........................................................................................................................... 159

CHAPTER 6 LEGAL SYSTEM IN ENGLAND & WALES (E&W) ................................................. 161

6.1 Introduction ............................................................................................................................. 161
6.2 Constitution in E&W ............................................................................................................. 161
6.3 Rule of Law in E&W ............................................................................................................. 163
6.4 Separation of Powers ............................................................................................................ 168
6.5 Judicial Independence .......................................................................................................... 171
6.6 Basic Criminal Law Principles in E&W ................................................................................ 174
   6.6.1 The Principle of Legality .................................................................................................. 174
   6.6.2 The Principle of Proportionality ..................................................................................... 176
   6.6.3 The Maximum Certainty Principle ............................................................................... 179
   6.6.4 The Non-Retroactivity Principle .................................................................................. 182
   6.6.5 The Principle of Minimalism ......................................................................................... 183
   6.6.6 The Harm Principle ..................................................................................................... 185
   6.6.7 The Principle of Normative Involvement .................................................................... 189
6.7 Conclusion .............................................................................................................................. 190

CHAPTER 7 LEGAL RESPONSES TO CYBERTERRORISM IN E&W ................................. 192

7.1 Introduction ............................................................................................................................. 192
7.2 Preventive and Pre-emptive Tendencies ............................................................................. 193
8.3.5 Aggravated Punishment for Terrorism-related Offences .......................................................... 269
8.3.6 Extension of Executive Powers ........................................................................................................... 270
8.4 Conclusion ............................................................................................................................................... 275

CHAPTER 9 CONCLUSION .......................................................................................................................... 277

9.1 Introduction ........................................................................................................................................... 277
9.2 Conjectures about the Convergence in Legal Responses to Cyber-terrorism in China and E&W .................................................................................................................................................. 277
9.2.1 Supra-national Demands for the Harmonisation of Counter-terrorism Law ........................................ 278
9.2.2 Demanding the Promotion of International Cooperation ........................................................................ 280
9.2.3 The Transfer of Anti-terrorism Law and Policy between Different Jurisdictions .............................. 282
9.3 Conjectures Explaining Divergence in Legal Responses to Cyber-terrorism in China and E&W ............................................................................................................................................................. 285
9.4 International Cooperation against Cyberterrorism ............................................................................... 287
9.5 An Evaluation of the Absence of Specific Legislation on Cyberterrorism ........................................... 292
9.6 Conclusion ............................................................................................................................................... 293

APPENDIX .................................................................................................................................................. 294

BIBLIOGRAPHY .............................................................................................................................................. 317
List of Legislation

Anti-Terrorism Proclamation 2009 (Proclamation No. 652/2009)
Anti-Terrorism, Crimes and Security Act 2001
Comment on Anti-Terrorism Proclamation 2009
Constitution of the People’s Republic of China
Constitutional Reform Act 2005
Council of Europe Convention on the Prevention of Terrorism
Counter-Terrorism Act 2008
Counter-terrorism and Border Security Act 2019
Counter-Terrorism and Security Act 2015
Counter-Terrorism Law of the People’s Republic of China
Criminal Attempts Act 1981
Criminal Law of the People’s Republic of China
Criminal Procedure Law of the People’s Republic of China
EU Framework Decision on Combating Terrorism of 2002,
European Convention on Human Rights
Explanatory Notes to TA 2006
Explosive Substances Act 1883
Firearms Act 1968
House of Commons Standing Order 152B.
Human Rights Act 1998
Intelligence Services Act 1994
Legislation Law of the People’s Republic of China
National Security Law of the People’s Republic of China
People’s Police Law of the People’s Republic of China
Prevention of Terrorism Act 2005
Public Order Act 1986
Rules of Criminal Procedure of the People’s Procuratorate of the People’s Republic of China
Serious Crime Act 2007
Terrorism Act 2000
Terrorism Act 2006
Terrorism Prevention and Investigation Measures Act 2011
The Council of Europe’s Convention on the Prevention of Terrorism 2005 and the Additional Protocol
The Council of Europe’s Cyber-Crime Convention 2001 and the Additional Protocol
UN International Covenant on Civil and Political Rights
## Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>APEC</td>
<td>Asia Pacific Economic Cooperation</td>
</tr>
<tr>
<td>ATCSA</td>
<td>Anti-Terrorism, Crimes and Security Act</td>
</tr>
<tr>
<td>CCP</td>
<td>China’s Communist Party</td>
</tr>
<tr>
<td>CECPT</td>
<td>Council of Europe Convention on the Prevention of Terrorism</td>
</tr>
<tr>
<td>CL</td>
<td>Criminal Law</td>
</tr>
<tr>
<td>COE</td>
<td>Council of Europe</td>
</tr>
<tr>
<td>CONTEST</td>
<td>Counter-Terrorism Strategy</td>
</tr>
<tr>
<td>CPL</td>
<td>Criminal Procedure Law</td>
</tr>
<tr>
<td>CRA</td>
<td>Constitutional Reform Act</td>
</tr>
<tr>
<td>CSIS</td>
<td>Centre for Strategic and International Studies</td>
</tr>
<tr>
<td>CTBSA</td>
<td>Counter-Terrorism and Border Security Act</td>
</tr>
<tr>
<td>CTC</td>
<td>Counter-Terrorism Committee</td>
</tr>
<tr>
<td>CTED</td>
<td>Counter-Terrorism Committee Executive Directorate</td>
</tr>
<tr>
<td>CTL</td>
<td>Counter-Terrorism Law</td>
</tr>
<tr>
<td>CTS</td>
<td>Critical Terrorism Studies</td>
</tr>
<tr>
<td>CTSA</td>
<td>Counter-Terrorism and Security Act 2015</td>
</tr>
<tr>
<td>DIA</td>
<td>Defense Intelligence Agency</td>
</tr>
<tr>
<td>E&amp;W</td>
<td>England &amp; Wales</td>
</tr>
<tr>
<td>ECHR</td>
<td>European Convention on Human Rights</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FATF</td>
<td>Financial Action Task Force</td>
</tr>
<tr>
<td>FBI</td>
<td>Federal Bureau of Investigation</td>
</tr>
<tr>
<td>FTF</td>
<td>Fusion Task Force</td>
</tr>
<tr>
<td>G-8</td>
<td>Group of 8</td>
</tr>
<tr>
<td>HRA</td>
<td>Human Rights Act</td>
</tr>
<tr>
<td>HRW</td>
<td>Human Rights Watch</td>
</tr>
<tr>
<td>IAEA</td>
<td>International Atomic Energy Agency</td>
</tr>
<tr>
<td>ICCPR</td>
<td>International Covenant on Civil and Political Rights</td>
</tr>
<tr>
<td>IMPACT</td>
<td>International Multilateral Partnership against Cyber Threats</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunication Union</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Name</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>JCHR</td>
<td>Joint Committee on Human Rights</td>
</tr>
<tr>
<td>NATO</td>
<td>North Atlantic Treaty Organization</td>
</tr>
<tr>
<td>NCTLO</td>
<td>National Counter-terrorism Leading Organ</td>
</tr>
<tr>
<td>NPC</td>
<td>National People’s Congress</td>
</tr>
<tr>
<td>OECD</td>
<td>Organization for Economic Co-operation and Development</td>
</tr>
<tr>
<td>PLC</td>
<td>Political and Legal Committee</td>
</tr>
<tr>
<td>POAC</td>
<td>Proscribed Organizations Appeal Committee</td>
</tr>
<tr>
<td>PTA</td>
<td>Prevention of Terrorism Act 2005</td>
</tr>
<tr>
<td>SCNPC</td>
<td>Standing Committee of the National People’s Congress</td>
</tr>
<tr>
<td>SPC</td>
<td>Supreme People’s Court</td>
</tr>
<tr>
<td>SPP</td>
<td>Supreme People’s Procuratorate</td>
</tr>
<tr>
<td>TA</td>
<td>Terrorism Act</td>
</tr>
<tr>
<td>TPIM</td>
<td>Terrorism Prevention and Investigation Measure</td>
</tr>
<tr>
<td>TPIMA</td>
<td>Terrorism Prevention and Investigation Measures Act 2011</td>
</tr>
<tr>
<td>UNCTITF</td>
<td>United Nations Counter-Terrorism Implementation Task Force</td>
</tr>
<tr>
<td>UNHCHR</td>
<td>United Nations High Commissioner for Human Rights</td>
</tr>
<tr>
<td>UNODC</td>
<td>United Nations Office on Drugs and Crime</td>
</tr>
<tr>
<td>UNSCR</td>
<td>United Nations Security Council Resolution</td>
</tr>
</tbody>
</table>
Figures

Figure 4.1: China’s Political Structure: The Communist Party sits atop China’s political power structure, controls all legislature, executive and judicial institutions, and commands the military. ..................................................................................................................................................................................... 79

Figure 4.2: key factors of ‘rule of law’ vs. ‘rule by law’ and implications of anti-terrorism laws in E&W and China. .................................................................................................................................................................. 83

Figure 4.3: Pyramid of Strategies of Responsive Regulation......................................................102

Figure 8.1: comparison of designation procedure of proscribed terrorist organizations in E&W and China...........................................................................................................................................................................268
Abstract

In response to the perceived threat of “cyberterrorism”, authorities in China and England & Wales (E&W) have not defined specific anti-cyberterrorism laws. Rather, they have relied on existing anti-terrorism legislation to combat this problem, leaving the legal definition of cyberterrorism ill-defined and open to significant interpretation. In turn, this grants substantial discretion to enforcement authorities which is a significant indicator of convergence in legal responses to cross-jurisdictional threats, even in legal systems as different as those in China and in E&W. Such convergence provokes the key question of whether a country's legal system necessarily shapes its legal response to social problems, particularly those arising from the 'hyper-connection' of human relations through the World Wide Web. To answer this question, this thesis compares the legal responses to cyberterrorism in China and E&W. The radical differences in the constitution of these two legal systems provide a ‘critical test’ of the necessary or contingent relationship between legal systems and legal responses in an era characterized by the increasing global problems facilitated by the World Wide Web.

To this end, the thesis adopts doctrinal, comparative and socio-legal methodologies to critically and comprehensively examine legal responses to cyberterrorism in these two systems. It is unsurprising there are many fundamental differences in legal responses to cyberterrorism, specifically the different judicial review process, different legislative scrutiny and independent review systems and different safeguards for the rights of terrorist suspects, which can be attributed to the differences in legal and political systems in the two jurisdictions. However, on closer analysis, there are a number of key similarities in their approaches, notably over-criminalization, unpredictability, lack of counterbalance, violation of proportionality and an ill-defined and arbitrary expansion of executive powers. This suggests there is no simple causal relationship between the constitution of these two legal systems and legal responses to cyberterrorism in these two jurisdictions. Rather, the revelation of this convergence in legal responses to cyberterrorism provokes key questions for further research on the socio-legal dynamics behind convergence as well as divergence in legal responses to global threats. In these terms, the thesis concludes by advancing a number of conjectures about the contingent, rather than necessary, relationship between legal systems and legal responses and the related significance of the extra-legal effects of
processes of globalization, including the ‘hyperconnectivity’ of communications through Web 2.0, and their challenges to national jurisprudence.
Chapter 1 Introduction

1.1 Research Background

Transnational Terrorism has become a phenomenon that threatens the stability, peace and security of countries around the world, and is something from which neither China nor England & Wales (E&W) are immune.¹ With the continuous development of network technology, traditional terrorism is quickly migrating to cyber space, where cyberterrorism emerges as a new global threat.² Compared to physical terrorism, cyberterrorism is a relatively new phenomenon which inflicts physical and virtual damage upon social networks and critical infrastructure all over the world, with such terrorists making use of the transnationality, convenience and anonymity afforded by cyber space.³ The threat of this newly-emerging cyberterrorism is generating a “legislative wildfire” amongst governments the world over who are enacting legislation to help detect, prevent, prosecute and eradicate it.⁴

There has been a substantial amount of literature on the concept of cyberterrorism.⁵ The definition of cyberterrorism could be generally categorized into two types: broad

⁴ M Clarke, Terrorism and Counter-terrorism in China: Domestic and Foreign Policy Dimensions (Oxford University 2018) 14.
⁵ This could be found in Chapter 2, section 2.2.
and narrow. The narrow definition refers to cyber attacks conducted via or against the Internet and/or national infrastructure (target-oriented cyberterrorism), while the broad definition concerns any cyber behavior on the Internet by terrorists (tool-oriented cyberterrorism). There is no controversy surrounding cyberattacks being regarded as cyberterrorism. So the focus of the dispute here is whether ancillary cyber activities should be classified as cyberterrorism. These ancillary cyber activities include fundraising, training, propaganda, incitement, reconnaissance and communication via the websites, social media, and forums, among other avenues. For the purpose of this thesis, I mainly focus on critically examining how China and E&W apply their existing anti-terrorism legislation to combat ancillary cyberterrorist activities. In addition, in this thesis, I would argue that cyberterrorism should be defined according to some of the following basic requirements: motivation; intention; and harm. This implies that only cyberterrorist activities which have a terrorism intention and cause serious harmful consequences could be qualified as cyberterrorism.

The United Nations has been committed to establishing effective programmes to deal with terrorism, which it considers a serious threat to mankind. For example, shortly after 9/11, the United Nations Security Council formulated a series of resolutions and established the Counter-Terrorism Committee (CTC) to urge member states to criminalise a series of terrorism-related offences in their domestic law. In this vein, criminal law appears to be an important mechanism to combat terrorism. Anti-terrorism laws (including criminal laws) and policies around the world have proliferated and subsequently affected the relationship between the state and society. As exemplified in the comparison of China and E&W in this thesis, both responded swiftly and comprehensively to these resolutions and the further criminalisation of terrorism-

---

7 For example, Resolution 1373 requires member states to ensure that terrorism and terrorist financing are considered serious crimes in their domestic laws; Resolution 2178 requires member states to further ensure that a series of precursor terrorism-related offences are considered serious crime; Resolution 1624 calls on countries to criminalize incitement to terrorist acts. Details could be found in Chapter 9.
related offences. However, amid this high demand for the formulation and revision of anti-terrorism laws and policies, few countries have paused to assess their justifiability and effectiveness.

In light of this, neither China nor E&W have promulgated specific anti-cyberterrorism laws to deal with the new emerging threat of cyberterrorism, relying instead on existing anti-terrorism legislation to combat this problem, which raises a series of important problems concerning ill-defined the definitions of cyberterrorism and expanding the scope of existing terrorism legislation to cover cyberterrorism offences. Correspondingly, this also grants executive agencies broad discretion to enforce anti-terrorism laws to deal with cyberterrorism. These issues are significant driving forces behind the convergence of China and E&W in their legal responses when dealing with the transnational problem of cyberterrorism, even if these two jurisdictions have completely different legal and political systems. Such convergence provokes the key question of whether a country’s legal system necessarily shapes its legal response to social problems, particularly those arising from the ‘hyperconnection’ of human relations through the World Wide Web.

It might be assumed that a country’s legal response would depend on its political and legal background. For example, upon comparing the legal responses to terrorism in different countries, Kent Roach argued that all such responses reflected each country’s own particular history and legal, political and social cultures. Alati also argued that the domestic political structure, legal system, human rights culture, and geopolitics all influence the evolution of anti-terrorism measures. In the course of conducting a

---

10 See Chapter 5, 7 and 8.
14 D Alati, ‘Domestic Counter-terrorism in a Global Context: A Comparison of Legal and Political
critical examination of China’s anti-terrorism politics and legal approaches, Zhang claimed that the authoritarian features of China’s anti-terrorism framework was highly state-centred, meaning that China’s political and legal system framed its anti-terrorism approaches. 15 Furthermore, Lu Hong et al. argued that “the divergence of law enforcement in both countries indicates how one nation’s specific practice is essentially rooted in its unique context.”16 However, through a closer analysis and comparison of the legal responses to cyberterrorism in China and E&W, this thesis argues that the nature of a legal system does not necessarily determine the corresponding legal responses. There is no international consensus about definition of cyberterrorism. It is generally

In order to answer the key question presented above, this thesis compares the legal systems for, and legal responses to, cyberterrorism in China and E&W to discern whether they are shaping domestic legal responses to cyberterrorism. E&W applies the rule of law (which means the supremacy of law, separation of powers, and judicial independence),17 while China applies ‘rule by law’, which means the supremacy the power of the Chinese Communist Party (CCP) and concentration of power, and a lack of judicial independence. 18 The stark differences between the legal and political systems of China and E&W make these two jurisdictions particularly amenable for this analysis, which provides a ‘critical test’ of the proposition that legal systems determine legal responses even when it comes to global problems, such as cyberterrorism.

To this end, the thesis adopts doctrinal, comparative and socio-legal methodologies to critically and comprehensively examine legal systems and legal responses to cyberterrorism in both jurisdictions. In particular, this research critically examines the legal responses of China and E&W to cyberterrorism, mainly by referring to existing criminal law, anti-terrorism laws and criminal procedure laws which have been applied to deal with cyberterrorism, paying particular regard to their legal principles. One might

---
17 See Chapter 6.
18 See Chapter 4.
assume that a liberal democracy will adopt a response that takes into account civil liberties, whereas an authoritarian regime would adopt an approach that does not pay heed to civil liberties. So unsurprisingly, we observed that there were indeed many fundamental differences in their legal responses to cyberterrorism, such as in their judicial review processes, legislative scrutiny and independent review systems, as well as varying safeguards for the rights of suspected terrorists, which are driven by the differences in the legal and political systems in the two jurisdictions. However, through in-depth and exhaustive analysis and comparison, we found that China and E&W shared a number of similarities in their legal responses to cyberterrorism, including the following: a tendency towards prevention and pre-emptive actions; broad and vague definitions of terrorism; criminalisation of a wide range of terrorism precursor offences; broad discretion of executive organs to designate proscribed terrorist organisations; aggravated punishment for terrorism; national security priority over human rights protection; and expansion of executive power. 19 With this in mind, I contend that the State’s legal response to cyberterrorism is not determined by the legal and political nature of the jurisdiction in question.

These convergences and divergences suggest that there is no simple causal relationship between the constitution of these two legal systems and legal responses to cyberterrorism in these two jurisdictions. So the substantive relations of connection between a legal system and the corresponding legal responses to cyberterrorism is not necessary but, rather, contingent because the problems (ill-defined, disproportionate, uncertain, lack of counterbalance, arbitrariness, expansion of executive powers) in legal responses to cyberterrorism are not necessarily the product of the ‘rule by law’ systems, but are instead contingent as such responses can also exist in ‘rule of law’ systems. 20 This implies that there are other key causal mechanisms at play, such as the need to adapt legal responses to the kind of fast-moving, potentially catastrophic, and cross-jurisdictional threats generated by the hyperconnectivity of the World Wide Web and epitomised by the problem of cyberterrorism.

19 Details could be found in Chapter 8, section 8.3.
20 See Chapter 8.
Accordingly, if both a rule of law system and a ‘rule by law’ system are capable of producing the abovementioned same problems in the legal responses to cyberterrorism, neither are necessary for the production of such responses. Therefore, what might be necessary for the production of such responses (e.g. hyperconnectivity threats that are so catastrophic they ‘necessitate’ pre-emptive or ‘precautionary’ legal responses jeopardizing, in turn, the retrospective establishment of guilt beyond all reasonable doubt, on the facts and after the facts that is central to due process in the rule of law) becomes a key question for further research in this field. This finding stimulates various conjectures for further research regarding what other factors could explain convergence as well as divergence in legal responses to global challenges such as cyberterrorism.21

1.2 Research Objectives and Questions

This thesis is a comparative study of legal responses to cyberterrorism of China and E&W, to establish whether the relationship between legal systems and legal responses is necessary or contingent in the case of counter-cyberterrorism. In pursuit of this, the objectives of the thesis are to:

- Map out and compare the basic distinctive characteristics of the legal systems of China and E&W (which are characterised in terms of a contrast between ‘rule by law’ and rule of law), and basic criminal principles (e.g. principles of proportionality, certainty, minimal criminalisation, and legality)
- Critically and comprehensively examine the basic principles of the legal responses to the perceived threats of cyberterrorism in China and E&W;
- Identify, through comparative analysis, any convergence as well as divergence in the legal responses to cyberterrorism in China and E&W;
- Clarify the analytical significance of differences in legal systems in explaining the legal responses to cyberterrorism, shifting the comparative focus from describing similarities and differences towards trying to understand what is necessary and contingent in the case of the relationship between legal system and legal

---

21 Details could be found in Chapter 9, section 9.2.
responses to cyberterrorism (e.g. a ‘rule by law’ system does not necessarily produce the problems of ill-defined, arbitrariness, uncertainty and disproportionality in legal responses to cyberterrorism because such responses also exist in a rule of law system); and

- Conjecture what else might account for patterns of similarity as well as difference in legal responses to cyberterrorism in China and E&W.

1.3 Originality and Contribution

This thesis seeks to explore the relationship between legal systems and legal responses to cyberterrorism. In addition, this thesis also attempts to analyse, critique, evaluate and compare existing strategies and legal responses to cyberterrorism in China and E&W. With this in mind, the contribution of this thesis to terrorism research can be demonstrated in several dimensions.

Firstly, this thesis contributes by originally posing the formal argument that the relationship between a legal system and legal responses to cyberterrorism in terms of the substantive relations of connection is not necessary but contingent, rather than describing formal relations of similarities and differences in legal responses to cyberterrorism. The comparative study of legal responses to cyberterrorism in China and E&W has been relatively uncommon, while, especially there has been no research at all to focus on critically analysing and exploring the relationship between the legal system and legal responses to cyberterrorism in China and E&W. In light of this, this thesis fills a significant gap in this field.

There has been some literature on the relationship between the legal system and the legal response to terrorism, and some studies have claimed that the legal system shapes the legal response. For example, Kent Roach argued that constitutional norms, local conditions, and geo-historical and cultural relations were significant driving forces behind divergences in counter-terrorism law across different jurisdictions. Meanwhile, Daniel Alati argued that the domestic political structure,
legal system, human rights culture, and geopolitics all influence the evolution of anti-terrorism measures. 24 Elsewhere, Zhang Chi argued that China’s anti-terrorism policies and legal approaches reflected the authoritarian features of China’s legal system, which is heavily state-centred. 25 Accordingly, Zhang’s viewpoint implied that China’s political and legal system framed its anti-terrorism approaches. Some work has conducted a comparative analysis of legal responses to terrorism in common law jurisdictions (such as E&W, the US and Canada), in which a lot of similarities could be observed, such as the vague and broad definition of terrorism, extensive legislation criminalising terrorism, a tendency to rely on existing criminal laws to combat terrorism, expansion of investigation powers, the extension of detention of suspected terrorists without charge, criminalisation of new offences, and imposing harsher sentences. 26 By analysing terrorism cases, it could be concluded that the legal principles of the major common law jurisdictions are similar when dealing with this transnational problem. 27 However, it is also worth noting that much of the literature has focused on analysing the legal responses to terrorism in common law systems or the Commonwealth legal systems, and the impact of such legal systems on anti-terrorism legislation. However, the comparative study of terrorism law been relatively scarce. Notably, China’s legal response to cyberterrorism has received little academic attention, particularly the comparative study of legal responses to cyberterrorism in China and E&W.

Therefore, in this research, I have selected two representatives of completely different legal systems: China (authoritarian regime) and E&W (democratic regime). Through a critical and comprehensive analysis of how they use existing anti-terrorism laws to combat cyberterrorism, unexpectedly, we found that there are many similarities in their legal responses to cyberterrorism. 28 These divergences and convergences highlight

---

28 See Chapter 8, section 8.3.
the importance of this thesis — the differences in legal systems cannot automatically explain legal responses to cyberterrorism.

Secondly, the originality of this research stems from its methodology. Doctrinal, comparative and socio-legal methods are employed to achieve the research aim, which implies not only technical examination of the texts of the laws relating to cyberterrorism, but also the evaluation of them within the legal system and basic principles, and integrating the socio-legal approach to explore how existing anti-terrorism laws are applied to combat cyberterrorism in practice in both jurisdictions. It is very rare for scholars to use a combination of doctrinal, comparative and socio-legal methodologies to provide a genuinely holistic overview of this issue. Some scholars use just use doctrinal methodology to study the definition of cyberterrorism and the existing legal responses to and strategies on cyberterrorism. Some of the literature has applied comparative methodology to study the definitions and legislation pertaining to anti-terrorism in common law systems and Commonwealth nations. Some works, meanwhile, have employed socio-legal and comparative methodologies to argue that political structure, legal system and human rights culture all influence anti-terrorism legislations.

In this thesis, doctrinal methodology is applied to describe the knowledge of existing anti-cyberterrorism strategies and legal responses in China and E&W. In addition, the materials for this study are mainly legislative sources, such as relevant provisions in Terrorism Acts(TA) in E&W, and Criminal Law(CL), Counter-Terrorism Law(CTL) and Criminal Procedure Law(CPL) in China, etc. Other materials such as court decisions, journal articles, NGOs reports, news reports, and official government reports are also considered. Comparative methodology is employed to figure out the formal relations pertaining to the similarities and differences of the legal systems and legal responses to cyberterrorism in China and E&W. Therefore, this thesis is dedicated to comparing the legal systems, political systems and specific legal responses to cyberterrorism

---

29 See Chapter 3, section 3.2, 3.4.
30 See Chapter 3, section 3.3.
31 See Chapter 3, section 3.3.
32 See Chapter 2, section 2.2.
33 The details could be found in Chapter 2.
34 See Chapter 2, section 2.3.
between China and E&W, and deriving convergences and divergences from them. Socio-legal methodology is adopted to explore whether the substantive relations of connection between legal systems and legal responses to cyberterrorism is contingent rather than necessary.\(^{35}\)

Thirdly, although the counter-terrorism legal approaches applied by E&W have been studied in great detail,\(^{36}\) this thesis provides the first comprehensive and critical analysis and comparison of the relationship between legal systems and legal responses to cyberterrorism in China and E&W. In addition, this thesis broadens the availability of research into legal responses to cyberterrorism available in the English language.

Moreover, there has been a lack of in-depth and critical research on legal responses to cyberterrorism in China. Most of the literature on cyberterrorism in China has focused on describing of the definitions, characteristics, typologies, development, and perceived threats of cyberterrorism.\(^{37}\) Additionally, relevant research on cyberterrorism is highly repetitive with little differentiation between the arguments presented by Chinese researchers working on this topic. This self-alignment and self-censorship limits Chinese academic criticism of existing legal responses to cyberterrorism. Most of these scholars have served to justify China’s counter-terrorism policies and legal responses, rather than critically challenge the existing authorities and problems, and as a consequence their studies reinforce existing anti-terrorism strategies in China.\(^{38}\)

Accordingly, this thesis makes the considerable contribution of a critical examination of existing anti-terrorism legislation in terms of basic principles of proportionality, certainty, minimal criminalisation, and so forth, in turn identifying tendencies that challenge a rule of law jurisprudence, such as: pre-emptive justice; broad and vague definitions; overcriminalisation of terrorism-related precursor offences; punitive strategy; expansion of executive powers; and arbitrariness.

\(^{35}\) See Chapter 2, section 2.4.
\(^{36}\) The details could be found in Literature Review Chapter 3, section 3.4.
\(^{37}\) Ibid.
\(^{38}\) The details could be found in Literature Review Chapter 3.
This thesis argues that the authoritarian characteristics of China’s legal response to cyberterrorism limit the CCP’s ability to strike a proper balance between effective counter-terrorism and protecting citizens’ rights as entitled by the Chinese Constitution. Like E&W, the democratic state, China has also begun to stress that anti-terrorism strategies should follow the law. However, faced with the more urgent need for national security and social stability, the CCP has been unrestricted in implementing heavy-handed counter-terrorism measures at the expense of civil rights. Given the curtailment of civil liberties, China's counter-terrorism approach is categorised as typically authoritarian. Recent reports on vast expenditure on public security, mass surveillance, and increased police presence, have further demonstrated the authoritarian characteristics of China's counter-terrorism approach. China is under pressure to maintain the legitimacy of its often-abusive counter-terrorism regime. The development of its counter-terrorism legal framework reveals a conflict between the pressure to comply with international norms and the single-party regime’s intrinsic need to consolidate power by curtailing civil liberties. For instance, the revision of the definition of terrorism in Counter-Terrorism Law (CTL) reveals just how limited the attempts have been to comply with international standards. In addition, the CCP reinforces the assumption that collective interests come before individual interests – only by expanding state power to control terrorism can citizens enjoy stability and physical security. The further curtailment of civil liberties in the name of anti-terrorism seems to be justifiable. However, given the lack of effective independent judicial review, very little can be done to prevent the abuse of executive power.

---

43 The initial draft of the law criminalizes “thoughts”, conflates terrorism and separatism, and is highly political and state-centric. The revised definition shows some limited attempts to conform to international standards by deleting “thoughts”, and adding an individual dimension into the definition of terrorism. This change indicates some awareness among political elites about the problems with the initial draft, and some attempts to shift the focus from state security to individual rights by complementing the state-centric counter-terrorism strategy with a dimension of human security on a normative level.
Fourthly, another contribution of this thesis is to show whether there is a ‘rule by law’ tendency emerging in E&W to use existing anti-terrorism legislation to combat cyber terrorism in E&W. Although E&W and China’s legal systems are completely different, there is some convergence in their legal responses to cyberterrorism. This means that E&W's approaches to cyberterrorism may jeopardise its adherence to the rule of law and have certain risks leading to rule by law. However, due to legal constraints such as an independent judiciary, independent review, and legislative scrutiny, in E&W there do remain some restrictions on state power and some protection of citizens' rights. It might nevertheless be opined that China's approach to tackling cyber-terrorism should not be criticised by Western jurisdictions like E&W, because E&W takes a substantially similar approach, and while at least China’s approach is in keeping with the spirit of its political and legal system, the E&W approach is at odds with its political and legal system.

The final claim of the originality made by this research is that this thesis also offers some conjectures which might explain the above-described similarities and differences, and which suggest an agenda for further research. For example, the factors in explaining the convergence of legal responses to cyberterrorism in different jurisdictions includes: convergence in supra-national demands for the harmonisation of counter-terrorism law to address trans-national issues; the promotion of international cooperation; and the transfer of anti-terrorism law and policy between different jurisdictions. Additionally, the interdependence of the global economy and related policy shifts are also factors influencing the convergence of legal responses to cyberterrorism. Meanwhile, the differences in legal approaches of different jurisdictions in response to global threats stem from: resistance from ‘net importers’ of legal responses originating in other nation-states; and political power in the competition amongst rival, multiple-centres of governance both within as well as between nation-states and their jurisdictions of sovereign writ.

1.4 Research Justifications

---

44 See Chapter 9.
45 The details could be found in Chapter 9, section 9.2.
46 See Chapter 9, section 9.3.
Firstly, there is a considerable amount of literature to have explored how legal responses to the threat of terrorism pose a threat to individual rights and liberties. Pertinently, it is worth questioning whether such legal responses are driven by the nature of the legal system in question. Some scholars have focused on British Commonwealth countries or common law systems to study the relationship between legal systems and legal responses to terrorism. Less common, however, are comparative studies looking at completely different legal systems and legal responses to terrorism, especially dealing with dealing with the transnational issue of cyberterrorism, let alone discussing the relationship between them. Therefore, in this thesis, I select two representatives of completely different legal systems, China (authoritarian regime) and E&W (democratic regime)\(^\text{48}\), which are justifiable to explore the relationship between a legal regime and legal responses to cyberterrorism. This thesis puts forward a hypothesis that because the autocratic regimes have less restrictions on administrative power, protects national security and collective interests, thereby ignores individual rights, so its legal response to cyberterrorism is fundamentally different from that of democratic countries that restrict state power to protect individual rights. Therefore, China and E&W have quite different regime types and also have significant differences in terms of legal, cultural, and political attributes, which have important implications on their choice of different approaches and laws to deal with cyberterrorism in the two jurisdictions.

China and E&W have very different legal systems, political systems, and constitutional traditions. E&W applies the rule of law (which means the supremacy of law), and China applies ‘rule by law,’ which means the supremacy of the CCP’s power and that the law is used as a tool to achieve the Party’s goals. The implication here is that China is an authoritarian state whose power is monopolised by the CCP, and since the rule of law will obstruct the ultimate authority of the CCP, the authoritarian state itself would not accept the Western rule of law under any circumstances, including separation of powers, judicial independence, and an independent legislative review system, among other aspects. On the one hand, some might consider such a disparity to render this

\(^{47}\) Details Could be found in Literature Review Chapter 3, section 3.4.

\(^{48}\) The details of definitions of autocracy and democracy could be find in Chapter 3, section 3.3.3.
comparative study untenable. Yet, as noted above, again, it is the radical difference between two systems, one premised on ‘rule by law’ and another on rule of law, that justifies this comparative study (given that the aim of the study is critically test the prevailing thesis in the existing literature that legal responses are driven by legal systems). Furthermore, what we find is that despite these constitutional differences, the outcomes are the same. Therefore, although China and E&W have different legal systems, politics, and constitutional principles, there has been some convergence in their legal responses to cyberterrorism.

Secondly, the analytical justification for the comparison is that both China and E&W are facing similar threats of cyberterrorism, and neither have a specific anti-cyberterrorism law to deal with it; rather, both simply apply their existing traditional terrorism laws when called to action. In addition, more powerfully and as noted above, the very different legal systems (rule by law vs. rule of law) in China and E&W allow for a critical test of the relationship between system and response. If such a causal relationship was true, then we would expect China and E&W to have similarly divergent legal responses to the problem of cyberterrorism.

However, through a critical examination and comparison of such legal approaches in China and E&W, it could be observed that they converge in certain areas in dealing with cyberterrorism (over-criminalisation; unpredictability; lack of counterbalance; violations of proportionality; ill-defined; arbitrariness; expansion of police power). These similarities are of great significance when explaining the relationship between a legal system and the legal responses.

1.5 Outline of Chapters

This thesis consists of nine chapters. This section aims to briefly set out the thesis’s structure and the content of each chapter.

Chapter two will provide a review of the existing literature on the relationship between

49 Details could be found in Chapter 8, section 8.3.
legal systems and legal responses, especially in the case of a shared, global problem such as cyberterrorism. This chapter will start with a literature review of the definition of cyberterrorism, which could be categorised into two types: broad and narrow. The narrow definition refers to cyberattacks conducted via or against the Internet and/or national infrastructure (target-oriented cyberterrorism), while the broad definition concerns any cyber behaviours on the Internet by terrorists (tool-oriented cyberterrorism). These ancillary cyber activities include fundraising, training, propaganda, incitement, reconnaissance and communications via the websites, social media, and forums, among other avenues. In this thesis, I mainly focus on the critical examination of how China and E&W apply their existing anti-terrorism legislation to combat ancillary cyberterrorist activities. Having considered the provenance and definitions of ‘cyberterrorism,’ the chapter then reviews the existing literature on the relationship between legal systems and legal responses to this problem. Here, the commonly held view among scholars that many legal systems do indeed determine legal responses is considered. In addition, this chapter also provides a literature review of prior critical examinations of the use of existing anti-terrorism laws to deal with cyberterrorism in China and E&W.

Chapter three will focus on the methodology. In this thesis, I will apply doctrinal, comparative and socio-legal methodology to achieve my research aim of ascertaining whether the relationships between legal systems and legal responses in the case of a cross-jurisdictional problem such as cyberterrorism is necessary or contingent. Doctrinal methodology is applied to figure out the distinctive characteristics of the legal systems in China and E&W, and the existing anti-cyberterrorism legislation and enforcement in both jurisdictions. A comparative method is used to explore the similarities and differences in the legal approaches in dealing with cyberterrorism between China and E&W. A socio-legal methodology is employed to explore whether the relationship between the legal system and legal responses to cyberterrorism in China and E&W is driven by formal legal processes, or by broader political and sociological factors.

Chapter four will explore some distinctive characteristics of the legal system in China, to fully explain its conceptualisation in terms of ‘rule by law’ and why this matters when
comparing legal responses to global uncertainties like cyberterrorism. Firstly, understanding of the ‘rule of law with Chinese characteristics’ contrasts sharply with the “Western version” of the rule of law, to the point that it would be better to characterise the Chinese system as ‘rule by law,’ in which there is a lack of any separation of power between the judiciary, legislature and executive, a related lack of supremacy of law and substantive judicial independence, a lack of due process and effective judicial review (producing a certain arbitrariness in law-making and enforcement), and a consequent concentration of power in the hands of the CCP.

Secondly, this chapter also sets forth the basic principles of criminal law in China, which reflect the characteristics of ‘rule by law’ in dealing with cyberterrorism. Essentially, China puts the protection of national security, social stability and collective rights first. The lack of democratic oversight and scrutiny of anti-terrorism legislation may therefore result in the violation of rule of law jurisprudence, including: the principle of proportionality; certainty of law; equity before law; minimal criminalisation; and principles of legality, in particular those of *nullem crimen sine lege* ("no crime without law") and *nullapoena sine lege* ("no punishment without law").

Chapter five will critically examine the existing legal approaches to cyberterrorism in China in terms of the basic principles of ‘rule by law’ considered in chapter four. Firstly, this chapter commences with a consideration of the guiding principle of counterterrorism work, highlighting the Chinese state’s concern with collective interests, social stability and the emphasis on national unity. Secondly, the CCP’s enactment of vague and open-ended anti-terrorism legislation (e.g. the vague and overbroad definition of terrorism, the ever-expanding scope of designation of “terrorist activities”, and vague and uncertain criteria for measuring the penalties), which may result in arbitrariness and violations of the principle of certainty, is examined. Thirdly, the chapter assesses China’s counterterrorism legal framework, which still relies on a punitive strategy, for example, prioritizing national security and social stability over human rights protection or the provision of harsher punishments for terrorism-related offences, which challenges the principle of proportionality. Fourthly, China has adopted a preventive and pre-emptive strategy to fight cyberterrorism (e.g. criminalisation of a wide range of terrorism offences online and offline), which may contravene the principle of minimal criminalisation, and this chapter also inspects this issue. Fifthly,
the chapter looks at the enforcement of counter-terrorism legislation, in which the executive departments are granted expansive discretion (such as investigation, designation, detention, and control orders) during counterterrorism cases. Additionally, there is a tendency to use non-criminal disruption methods to deal with precursor terrorism-related offences. Finally, the chapter covers China’s counter-terrorism approach, which is constrained by authoritarian characteristics such as a lack of checks and balances protecting human rights and a lack of independent judicial review over executive powers when it comes to designating what constitutes terrorism and the consequent use of control orders.

Chapter six provides an overview of the legal system in E&W, underpinned by the rule of law, and its relationship to legal responses to cyberterrorism. Firstly, it explains that the rule of law, implies that no arbitrary power is placed in the hands of the state as there is a separation of powers between the executive, legislature and judiciary. Secondly, this chapter also elaborates upon the basic principles of criminal law-making in E&W, which reflect the “rule of law”. These basic principles (the principles of legality, proportionality, certainty, minimal criminalisation, and non-retroactivity) are then applied to evaluate the actual legal responses to cyberterrorism.

Chapter seven will comprehensively analyse and critically evaluate the existing legal approaches to combating cyberterrorism in E&W in terms of basic principles elaborated upon in the last chapter. Firstly, this chapter starts with the guiding principle of counterterrorism work, by quoting the comprehensive counter-terrorism strategy("CONTEST"), which emphasises the adoption of pre-emptive and preventive measures as a basis for countering terrorism. Secondly, the chapter considers the vague and over-inclusive definition of terrorism in E&W and how this has raised serious concerns about the violation of principles of legality and certainty. Furthermore, the wide-reaching definition of terrorism serves to further extend the reach of the criminal law through ‘preventive offences’ that criminalise acts of innocence or remote harm, which in turn violates the principle of minimal criminalisation. Thirdly, the chapter considers the way in which E&W, like China, has criminalised a wide range of precursor terrorism offences, consequently contravening principles of legality and minimal criminalisation. Fourthly, the chapter details how the executive departments have been
granted a wide discretionary power to designate the proscription of terrorist organisations. Fifthly, it outlines that terrorism-related offences have also attracted harsher punishment, which can violate proportionality, suggesting, in turn, that E&W has utilised a punitive strategy in response to the threat of terrorism. Additionally, with respect to the enforcement of anti-terrorism laws, a gradual extension of executive powers to interrogate, detain and control suspected terrorists during preliminary investigation or pre-charge periods is described.

Following on from the foregoing analysis, chapter eight highlights the convergences as well as divergences in legal responses to cyberterrorism between China and E&W. This chapter acknowledges that there are significant differences in legal responses to cyberterrorism that can be attributed to differences in legal and political systems. These include: a different judicial review process; different legislative scrutiny and independent review systems; and different safeguards for the rights of suspected terrorists. However, upon closer analysis, China and E&W share a number of similarities, suggesting that the nature of a legal system does not determine the legal responses to cyberterrorism. These commonalities can be divided into the following three categories: (1) substantive counter-terrorism laws (prevention and pre-emptive tendency, overbroad and vague definition of terrorism, wide range of precursor offences, and broad discretion of executive powers); (2) procedures for enforcing counter-terrorism laws (extension of executive powers to interrogate, detain, and control suspected terrorists); and (3) punishment of terrorism offences (aggravated penalties for terrorism). Ultimately, it is argued that differences in a legal system cannot explain these convergences in legal responses particularly to cross-jurisdictional problems for law enforcement, such as cyberterrorism.

Chapter nine concludes with conjectures regarding further research about convergence as well as divergence in legal responses to global challenges such as cyberterrorism. This thesis suggests that the convergence of legal responses to transnational threats in different jurisdictions might derive from: pressure from supranational institutions (such as the UN, or the EU) to harmonise anti-terrorism laws; demands for greater international cooperation; and the transplanting of anti-terrorism laws and policies from one jurisdiction to another. However, through further analysis, a
number of conjectures might explain the differences in anti-terrorism approaches of different states, including: differences in the prioritisation of national security and sovereignty amongst competing or conflicting strategic interests; different political, historical, cultural, and socio-economic conditions of jurisdictions; and resistance from “net importers” of legal responses originating in other nation-states. Furthermore, another implication of this thesis is the need for international cooperation to combat cyberterrorism. At present, there is lack of a special anti-cyberterrorism convention, so it is necessary to establish an international legal framework, reach international consensus and make global joint efforts to criminalize various forms of terrorist acts and exercise universal jurisdiction. There are some existing bilateral international or regional cooperation that can be used to combat cyberterrorism, such as the UN, Interpol and International Multilateral Partnership against Cyber Threats (IMPACT), etc.
Chapter 2 Literature Review

2.1 Introduction

This chapter comprises a review of the relevant literature on the concept of cyberterrorism, and the relationship between legal systems and the legal responses in this regard. A literature review can be described as ‘the foundation and inspiration for substantial, useful research.’\(^{50}\) Flink opined that: ‘A research literature review is a systematic, explicit, and reproducible method for identifying, evaluating and synthesizing the existing body of completed and recorded work produced by researchers, scholars and practitioners.’\(^{51}\) Building upon this, I seek to go further than previous studies by concentrating in depth on selected issues and by producing not just an evaluation of existing anti-cyberterrorism legislation in China and E&W, but comparing their respective legal systems and legal responses.

This chapter starts by discussing the definition of “cyberterrorism.” Although a substantial amount of literature has been written on the concept of cyberterrorism, and some international or regional organizations have defined cyberterrorism (such as NATO and COE), it is not accepted by the domestic laws of all countries. For example, the domestic laws of China and E&W do not provide the definition of cyberterrorism. Definitions can generally be divided into two types: narrow and broad. A narrow definition only focuses on cyberattacks, while a broad definition also encompasses any cyberterrorist activities using the Internet as a tool. In this thesis, I mainly focus on critically examining how China and E&W apply their existing anti-terrorism legislation to combat ancillary cyberterrorist activities. Pertinently, ancillary cyberterrorist activities could also be classified under cyberterrorism, but for the purposes of this thesis only the cyber terrorist activities which have terrorism intentions and/or cause serious harmful consequences are considered as cyberterrorism.

Thereafter, this chapter moves on to review the previous literature on the relationship


\(^{51}\) A Flink, Conducting A Research Literature Review: From Internet to Paper (Sage 2010) 3.
between legal systems and cyberterrorism. Much of the literature has argued that a legal system frames the legal response to terrorism. Meanwhile, compared to democracies, authoritarian states are more adept at suppressing and preventing terrorism because they are less constrained by democratic values.

This chapter then provides a review of the literature to have critically examined the use of existing anti-terrorism laws to deal with cyberterrorism in China and E&W. The current legal approaches to cyberterrorism have been subjected to considerable criticism, mainly focusing on the tension between the imperative of prevention, expanding the boundaries of criminal liability and the subsequent impact on human rights, as well as the rule of law. However, in China the close ties between academia and officialdom prevents scholars from making critical analysis that may be considered hostile by government officials. Instead, they tend to follow the official discourse (such as prioritising safety, prevention and extension of criminal liability, and aggravated punishment).

2.2 Defining “Cyberterrorism”

In order to understand legal responses to cyberterrorism, some basic concepts in cyberterrorism studies need to be clarified. As Weimann noted, ‘……if we want to clearly understand the threat posed by cyberterrorism, we must define it precisely.’52 There is no international consensus about the definition of cyberterrorism. Indeed, even in the same country the definitions may vary. For instance, in the USA, the definition of cyberterrorism varies in different departments.53 Ultimately, defining the scope of cyberterrorism is an extremely difficult task, and scholars have canvassed it from different angles.54

It is generally accepted that the term "cyberterrorism" was first coined by Barry C. Collin in 1997, who was referring to the convergence of terrorism and cyberspace. However, the potential threat of cyberterrorism had not yet been fully identified at that time. Even a decade later, the Defense Intelligence Agency (DIA) noted: ‘Cyberterror is not a threat. At least not yet, and not for a while.’ Now, an increasing number of researchers are paying attention to the threats posed by cyberterrorism, underpinned by a widespread view that such threats are growing. Schudel et al. raised concerns about the threats to critical infrastructure from cyberterrorists. Elsewhere, Jarvis, Nouri and Whiting noted ‘although [cyberterrorism as a term] has existed for over 30 years now, there remains very little consensus on many of the fundamental questions surrounding this term.’ Since Collin’s vivid description of cyberterrorism and cyberattacks, with the continuous emergence of hacker behaviour around the world, the word "cyberterrorism" started to attract people's attention.

Although scholars have studied the subject for more than two decades, due to its complexity, dynamics and multi-faceted nature, there is still no universally accepted definition of cyberterrorism, and even there is no official definition of cyberterrorism in China and E&W. Furthermore, Brickey claimed that one reason why cyberterrorism is difficult to frame uniformly is that the terms “cyberwar,” “cyberterrorism,” “cybercrime,” and “hacktivism” are often misunderstood and conflated by the media and/or public.

According to Brunst:

56 B Nelson, R Choi, M Iacobucci, M Mitchell and G Gagnon, Cyberterror: Prospects and Implications (Storming Media 1999).4
A more narrow view is often worded close to common terrorism definitions and might include only politically motivated attacks against information systems and only if they result in violence against noncombatant targets...Broader approaches often include other forms of terrorist use of the Internet and therefore might define cyberterrorism as almost any use of information technology by terrorists.  

As alluded to earlier, the definitions of cyberterrorism generally could be divided into narrow or broad. The narrow definition seems to like concentrate only on cyberattacks (also referred to as target-oriented cyberterrorism) conducted via or against Internet, seeking to damage national critical infrastructures. Meanwhile, the broad definition not only includes cyberattacks, but also encompasses any cyber behaviours on the Internet carried out by terrorists (tool-oriented cyberterrorism). For instance, a cyberterrorism event may also sometimes depend on the presence of other factors beyond just the cyberattack itself. These ancillary cyber activities to which we refer here include fundraising, training, propaganda, incitement, reconnaissance and communications via a website, social media platform or forum. Talihärm also classified the definition of cyberterrorism in a similar way:  

The first identifies as cyberterrorism all politically or socially motivated attacks against computers, networks and information, whether conducted through other computers or physically, when causing injuries, bloodshed or serious damage, or fear (hereafter ‘target-oriented cyberterrorism’). The second labels all actions using the Internet or computers to organize and complete terrorist actions as cyberterrorism (hereafter ‘tool-oriented cyberterrorism’).  

---

63 Ibid.  
66 AM Talihärm, ‘Cyberterrorism: In Theory or in Practice?’ (2010) 3(2) DATR 59, 63-64.
Some scholars have however acknowledged that only cyberattacks themselves could be qualified as cyberterrorism.\textsuperscript{67} Under such a view, terrorists’ use of computers as a facilitator of their activities, whether for propaganda, recruitment, data-mining, communication, or other purposes, is not cyberterrorism.\textsuperscript{68} Perhaps the most famous and familiar example of the narrow approach was proposed within Dorothy Denning’s testimony in 2000 before the US House of Representatives, which read as follows:

> Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.\textsuperscript{69}

According to this definition, disrupting nonessential services does not count as cyberterrorism.\textsuperscript{70} Furthermore, to qualify as cyberterrorism, an attack should bring a certain level of physical harm against people, property or critical infrastructures. In addition, Denning also proposed the following concise definition of cyberterrorism: ‘Politically motivated hacking that intentionally causes serious harm (such as casualties or serious economic damage).’\textsuperscript{71}


\textsuperscript{68} G Weimann, ‘Cyberterrorism: The Sum of All Fears?’ (2005) 28 SCT 129, 132-133.

\textsuperscript{69} DE Denning, ‘Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services US House Representatives’ (Georgetown University, 10 October 2003 ) < http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html> accessed 21 May 2020; See also M Conway, ‘Cyberterrorism: Media Myth or Clear and Present Danger?’ in J Irwin(ed), \textit{War and Virtual War: the Challenges to Communities} (Rodopi 2004) 81-82.

\textsuperscript{70} DE Denning, ‘Cyberterrorism Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives’ in EV Linden(ed), Focus on Terrorism(Nova Publishers 2007) 71-76.

\textsuperscript{71} D Denning, ‘Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign
Compared to Denning, Weimann and Lewis, narrowed their definition down to ‘the use of computer network tools to harm or shut down critical national infrastructures (such as energy, transportation, government operations).’ However, Weimann also argues that threats posed by terrorists’ other uses of the Internet, ‘ranging from psychological warfare and propaganda to highly instrumental uses such as fundraising, recruitment, data mining, and coordination of actions.’ He didn’t mentioned whether these listed activities should be considered cyberterrorism. In addition, Conway followed Denning’s definition by introducing a requirement that offline damage had to be caused. Hua and Bapna, and Mark Pollitt, defined the term similarly, as ‘an activity implemented by computer, network, Internet, and IT intended to interfere with the political, social, or economic functioning of a group, organization, or country; or to induce physical violence or fear; motivated by traditional terrorism ideologies.’ Some other scholars have also agreed that the term “cyberterrorism” is used to describe the new approaches adopted by terrorists to attack cyberspace.

Some scholars or organizations define cyberterrorism by enumerating the categories of cyberterrorism activities. Jalil listed five types of cyberterrorist attack: incursion; destruction; disinformation; denial of service; and defacement of websites. Meanwhile, Zanini and Edwards classified three types of cyberterrorism: using the Internet for propaganda, fundraising, recruitment and influencing public opinion;
disrupting targeted systems; and destroying critical infrastructures.\textsuperscript{78} The Council of Europe (COE) has divided cyberterrorism into the following three different categories: attacks via the Internet; dissemination of content (such as propaganda, fundraising, recruitment and training); and use of the Internet for other purposes (e.g. individual communication, planning, and data mining).\textsuperscript{79} Moreover, the COE explained that due to characteristics of anonymity, convenience, efficiency, rapidity and cheapness, terrorist organisations prefer to use the Internet or other information technologies to conduct their terrorist activities.\textsuperscript{80}

By contrast, Ballard \textit{et al.} divided the typology of cyberterrorism into the following four categories: ‘information attacks; infrastructure attacks; technological facilitation; fundraising and promotion’.\textsuperscript{81} In addition, the UN highlighted the Internet as one of the most effective ways for terrorists to engage in communication, propaganda, fundraising and promotion.\textsuperscript{82} The UN specifically defines cyberterrorism into the following four categories:

1. Use of the Internet to remotely change information on computer systems or interfere with data communications between computer systems to carry out terrorist attacks;
2. using the Internet to collect information and obtain other resources through the Internet for the purpose of terrorist activities;
3. using the Internet as a means of publishing and disseminating terrorism-related information;
4. using the Internet to communicate and plan or support terrorist activities.\textsuperscript{83}

In addition, the current North Atlantic Treaty Organization (NATO) definition of cyberterrorism is: “A cyberattack using or exploiting computer or communication
networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal.”\textsuperscript{84} Due to its non-physical characteristics, NATO also recognizes that it is difficult to define an accurate definition of cyberterrorism. In addition, the Centre for Strategic and International Studies (CSIS) defined the cyberterrorism in 1998, suggesting that: “Cyber terrorism means premeditated, politically motivated attacks by subnational groups or clandestine agents, or individuals against information and computer systems, computer programs, and data that result in violence against non-combatant targets.”\textsuperscript{85}

Elsewhere, some scholars have also proposed other ways of defining cyberterrorism, with certain elements originating from the attack(s) (effects-based) and other elements originating from the attacker(s) (intent-based).\textsuperscript{86} Although they define cyberterrorism in different ways, they still generally accept a narrower definition. Hardy and Williams claimed that the definition of cyberterrorism includes an intention requirement, a motive requirement, or a harm requirement, and that these requirements are useful to apply when identifying a cyberattack.\textsuperscript{87}

\subsection*{2.2.1 Literature Review of Definitions of Cyberterrorism in China}

Chinese scholars took longer to engage in cyberterrorism research compared to their Western peers. This is largely because the rise of cyberterrorism in China and its emergence as a threat to the public and the Chinese government originated as recently as 2014.\textsuperscript{88} Another reason for this apparent tardiness is that cyber terrorist activities...

\textsuperscript{84} Centre of Excellence Defence Against Terrorism, \textit{Responses to Cyber Terrorism} (IOS press, 2007) 119.
\textsuperscript{86} Effects-based: Cyber terrorism exists when computer attacks result in effects that are disruptive enough to generate fear comparable to a traditional act of terrorism, even if done by criminals.
• Intent-based: Cyber terrorism exists when unlawful or politically motivated computer attacks are done to intimidate or coerce a government or people to further a political objective or to cause grave harm or severe economic damage. See J Rollins and C Wilson, ‘Terrorist capabilities for Cyber Attack: Overview and Policy Issues’ in EV Linden, \textit{Focus on Terrorism} (Nova Publisher 2007) 43-63; PM Tehrani, \textit{Cyberterrorism: The Legal and Enforcement Issues} (World scientific press 2017)301.
\textsuperscript{87} K Hardy and G Williams, ‘What is ‘Cyberterrorism’? Computer and Internet Technology in Legal Definitions of Terrorism’ in TM Chen, L Jarvis and S Macdonald(eds), \textit{Cyberterrorism: Understanding, Assessment, and Response} (Springer 2014) 5.
depend on the development and application of Internet technology, which happened more slowly in China than it did in the likes of the USA or the UK. Moreover, to defend China’s “cyber sovereignty,” the CCP has taken a long-lasting strategy of ‘special action against online terrorist audio and video and the Great Firewall’\(^\text{89}\), which has created an environment in which the public would struggle to obtain terrorism-related materials and has little access to accounts that are not officially verified/endorsed by the State.\(^\text{90}\) By doing so, the CCP has been able to legalise its preventive and pre-emptive strategies to respond to cyberterrorism, which is to reduce the threats posed by radicalisation to national security and social stability.

Given these circumstances, many Chinese scholars have directly quoted or imitated the definitions of cyberterrorism presented by Western scholars or institutions. For example, Pi Yong\(^\text{91}\) adopted the United Nations Counter-Terrorism Implementation Task Force’s (CTITF) definition, but pointed out the ways in which any terrorist group may make ‘use of the Internet to perform terrorist attacks by remotely altering information on computer systems or disrupting the flow of data between computer systems.’\(^\text{92}\) To clarify, the CTITF rigorously restricted its definition, according to which only by causing loss of life or severe property damage in the offline world could an act be qualified as a cyberattack. Moreover, there is still tremendous controversy about cyberattacks only causing online interruption or economic losses being qualified as terrorism. At the same time, Zhu Yongbiao and Ren Yan have cited Denning’s definition

---

89 The Great Firewall of China (GFW) is the combination of legislative actions and technologies enforced by the PRC to regulate the Internet domestically. Its role in the Internet censorship in China is to block access to selected foreign websites and to slow down cross-border internet traffic, and also strengthen control over public opinions online within China. Reuters, ‘China launched a special action to eradicate audio and video of violent and terrorism on the Internet’ (Reuters, 20 June 2014) <https://www.reuters.com/article/china-anti-terror-av-material-idCNKBS0EV10520140620> accessed 5 Dec 2020.


92 The UNCTITF explains: “any cyberattack qualifying as ‘terrorist’ would ultimately still have to cause damage in the ‘real world’: for example, by interfering with a critical infrastructure system to the extent of causing loss of life or severe property damage. However, as dependence on online data and services increases, an attack that resulted only in widespread interruption of the Internet could, in future, cause sufficient devastation to qualify as a terrorist attack. However, categorizing such attacks as terrorist remains controversial. The damage resulting from such attacks, while potentially economically significant, to date their impact has been more on the level of a serious annoyance.” U.N. Counter-Terrorism Implementation Task Force, Report on ‘Working Group on Countering the Use of the Internet for Terrorist Purposes’ ( UN org, February 2009) <https://www.un.org/counterterrorism/ctif/sites/www.un.org.counterterrorism.ctif/files/ctif_internet_wg_2009_report.pdf> accessed 13 March 2020.
of cyberterrorism and only partially agreed that ‘cyberterrorism was the convergence of terrorism and cyberspace,’\textsuperscript{93} but unlike Denning, they adopted the broad definition of cyberterrorism.\textsuperscript{94}

Interestingly, the majority of Chinese scholars have adopted the broad definition of “cyberterrorism”, which includes both tool-oriented cyberterrorism (工具型网络恐怖主义) and target-oriented cyberterrorism (目标型网络恐怖主义).\textsuperscript{95} A few of Chinese scholars have applied the narrow definition of cyberterrorism, which refers to a premeditated and politically-motivated attack or act carried out by sub-state groups or clandestine organisations targeting information systems, computer systems, computer programmes and data.\textsuperscript{96}

China’s official position on cyberterrorism falls under its combating of any form of terrorism, which means that auxiliary cyberterrorist activities could fall into the category of cyberterrorism. Accordingly, the Chinese authorities crack down on cyberterrorism in a broad way, and cyberterrorism is regarded as a subset of terrorism.\textsuperscript{97} According to Wang Yi, China resolutely combats all forms of terrorism and is committed to strengthening international counter-terrorism cooperation, and increasing exchanges and mutual learning between experts, scholars and practitioners from various countries.\textsuperscript{98}

\textsuperscript{93} DE Denning, 'Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services US House Representatives' (Georgetown University, 10 October 2003) <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html> accessed 21 May 2020.

\textsuperscript{94} See Zhu Yongbiao and Ren Yan, Research on International Cyberterrorism (国际网络恐怖主义研究) (China Social Sciences Press 2014) 19-20.


\textsuperscript{97} Zhao Chen, ‘Cyberspace has become a new platform of international counter-terrorism’ (China’s Office of Central Space Affairs Commission (中共中央网络和信息化委员会办公室), 14 Jun 2017) <http://www.cac.gov.cn/2017-06/14/c_1121140970.htm> accessed 20 June 2020.

\textsuperscript{98} ‘The Second Symposium on Combating Cyber Terrorism under the Framework of “Global Counter-
Essentially, the majority of China’s scholars follow the official position and adopt a broad definition.\textsuperscript{99} This reflects the authoritarian characteristics of China’s approaches to countering cyberterrorism. The scholarly works written in the Chinese language are largely prescriptive, based on the assumption that all types of the terrorism-related Internet users are classified as cyberterrorists, as long as they seek to ‘damage national security, national unity, national economic construction, social public order, people’s life and property regardless of intent or negligence.’\textsuperscript{100}

\subsection*{2.2.2 Literature Review of Definitions of Cyberterrorism in E&W}

Neither China nor E&W have a clearly official definition of cyberterrorism. However, Terrorism Act 2000(TA 2000), s 1 provides E&W’s statutory definition of terrorism. It encompasses ‘politically-motivated behaviours designed to seriously interfere with or disrupt electronic systems.’\textsuperscript{101} This would include cyber-attacks on Internet service providers, financial exchanges’ computer systems, and controls of national power and water.\textsuperscript{102} Walker highlighted that ‘politically-motivated behaviours designed to seriously interfere with or disrupt electronic systems’\textsuperscript{103} was included to offer a legal outline of cyberterrorism, and to distinguish the dichotomy between ‘costly nuisances’ and bona fide ‘cyberterrorism.’\textsuperscript{104} This dichotomy also distinguishes between general hacking and serious cyberterrorist attacks.

Moreover, this definition of terrorism\textsuperscript{105} is sufficiently broad that it could be applied to cyberterrorists.\textsuperscript{106} Therefore, legislation is considered to represent E&W’s approach
to defining cyberterrorism.\textsuperscript{107} Moreover, the scope of the range of terrorism-related offences and designation of terrorist organisations have relied on the definition of terrorism.\textsuperscript{108} This means that individuals who use computers and Internet technologies in a way that ‘does not directly harm others may still be subject to severe penalties, such as for posting videos on YouTube that glorify terrorism.’\textsuperscript{109}

Lee Jarvis and Stuart Macdonald explored the definitional issues of cyberterrorism through a survey of 118 respondents from 24 countries, and found out some commonly perceived features of cyberterrorism, including: '(a) motive; (b) digital means or target; (c) fear as an outcome; and (d) political or ideological motivation'.\textsuperscript{110} This finding ran counter to the view of traditional terrorism, for which “violence” and “force” were the most prevalently mentioned features.\textsuperscript{111} Terrorists propagandise, incite, or publish terrorism-related materials via the Internet. These materials are easily accessible and widely available online.\textsuperscript{112} Moreover, cyberterrorists use of a combination of social media and official websites to engage in recruitment, propaganda and incitement of terrorism.\textsuperscript{113}

Cyberattacks launched by terrorists are listed as one of the four ‘highest priority risks’\textsuperscript{114} in the UK’s national security strategy. The strategy illustrates that cyberattacks on government, military, industrial, and economic targets may have ‘potentially damaging real-world effects.’\textsuperscript{115} Scholars are still divided as to controversial about

\textsuperscript{107} See further K Hardy and G Williams, ‘What is ‘Cyberterrorism’? Computer and Internet Technology in Legal Definitions of Terrorism’ in T Chen, L Jarvis and S Macdonald(eds), Cyberterrorism: Understanding, Assessment and Response (Springer 2014).
\textsuperscript{108} Details could be found in Chapter 7, section 7.5 and 7.6.
\textsuperscript{109} K Hardy and G Williams, ‘What is ‘Cyberterrorism’? Computer and Internet Technology in Legal Definitions of Terrorism’ in T Chen, L Jarvis and S Macdonald(eds), Cyberterrorism: Understanding, Assessment and Response (Springer 2014).
\textsuperscript{113} CA Theohary and J Rollins, Terrorist Use of the Internet: Information Operations in Cyberspace (DIANE Publishing 2011) 3.
\textsuperscript{114} Cabinet Office, The national security strategy: a strong Britain in an age of uncertainty(Cm 7953,2010) 11.
\textsuperscript{115} Ibid 30.
whether terrorists use computers or networks to launch such attacks.\textsuperscript{116} It is also worth noting that in addition to cyberattacks, terrorists also use the Internet to carry out activities such as fundraising, recruitment, propaganda, incitement and communication.\textsuperscript{117}

As following chapters illustrate, such uses of computers and the Internet for terrorism purposes fall under the statutory definition of “terrorism” in E&W. An analysis of such definitions is necessary because a range of criminal offences and other statutory powers that may have serious consequences for individuals depends on the definition of terrorism. This also serves as the starting point for an analysis of the definition of “cyberterrorism.”

I examine legal definitions of terrorism in two different regime types: China (authoritarian) and E&W (democratic). Although there are many differences between, their definitions of terrorism have many similarities. Exploring these similarities is valuable when discussing a wide range of issues in the legislation and the political discourse on how to define cyberterrorism.

Although there are other criminal offences regarding the use of computers in China and E&W, this thesis focuses on the definitions of terrorism and terrorism-related criminal offences, because this determines what acts can be considered as terrorism under each jurisdiction’s domestic law. There is no such offence as “cyberterrorism” in the jurisdictions of China or E&W, but this problem could still be addressed by exploring how the improper use of computers and the Internet would fall under each jurisdiction’s legal definition of terrorism.

\textsuperscript{116} See M Conway, ‘Hackers as Terrorists? Why it doesn’t Compute’ (2003) 12CFS 10–13; M Conway, ‘Reality Check: Assessing the (un)likelihood of Cyberterrorism’ in T Chen, L Jarvis, S Macdonald (eds), Cyberterrorism: Understanding, Assessment, and Response (Springer 2014); S Michael, ‘Cyber Terrorism: A Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Games?’ (2006) 46(4–5) CLSC 223, 229; The commonly agreed upon components which Stohl refers to are “some form of intimidate, coerce, influence as well as violence or its threat.”

Lord Cope of Berkeley explained that TA 2000, s1(2)(e) ‘extends the definition to cover what is known in the jargon as cyberterrorism.’\(^{118}\) The scope of preparatory offences rely upon this definition, and it also determines the availability of statutory powers for preventing terrorism and cyberattacks.

\(R v\) Gul\(^{119}\) is a typical case illustrating the extent to which E&W’s anti-terrorism laws regulate the use of computer and Internet technology for terrorism purposes. According to the offences deriving from the definition of terrorism, individuals who use technology in a way that does not cause any direct harm to others, such as uploading a video to a website, may still be severely imprisoned. These acts could fall into the broader heading of “cyberterrorism” because they involve the use of Internet technology for terrorism purposes which should be punished under E&W’s law.\(^{120}\)

E&W’s legislation has sufficient capacity to respond to cyberterrorism, but it may overreact, whereby legitimate online protests and forms of illegal hacking other than terrorism could also be targeted under the legislation.\(^{121}\) This may have serious implications for the rule of law and freedom of speech due to the broad discretion of statutory powers. Lord Carlile (then an independent reviewer) considered it was justifiable to apply s1(2)(e) because acts of cyberterrorism could cause serious physical and economic harm.\(^{122}\) In addition, after a comparative analysis of legal definitions of terrorism in the UK, Australia, Canada, and New Zealand, Hardy and Williams concluded that cyberterrorism meant conduct involving computer or Internet technology that:

(1) is motivated by a political, religious or ideological cause; (2) is intended to

\(^{118}\) HL Deb 16 May 2000, vol 613, col 230.
\(^{119}\) \(R v\) Gul [2012] EWCA Crim 280. In this case, a law student in the UK had uploaded videos onto YouTube of insurgents attacking Coalition forces in Iraq and Afghanistan. The videos were accompanied by statements praising the bravery of the insurgents and encouraging further attacks. The student received 5 years imprisonment for disseminating terrorist publications with intent to encourage terrorism.
\(^{121}\) K Hardy and G Williams, ‘What is ‘Cyberterrorism’? Computer and Internet Technology in Legal Definitions of Terrorism’ in TM Chen, L Jarvis and S Macdonald(eds), Cyber-terrorism: Understanding, Assessment, and Response (Springer 2014)1-23.
\(^{122}\) Carlile A, The definition of terrorism (Cm 7052, 2007) 40.
intimidate a government or a section of the public; and (3) intentionally causes serious interference with an essential service, facility or system, if such interference is likely to endanger life or cause significant economic or environmental damage.  

Apparently, the narrow definitions of cyberterrorism (such as those put forward by Denning and Weimann) are more prevalent and accepted by scholars than their more expansive alternatives in the Western academic literature. In contrast, China’s scholars are more inclined to adopt a broad definition of cyberterrorism. There is thus no controversy surrounding cyberattacks being regarded as cyberterrorism. The focus of the dispute here is whether ancillary cyber activities should be classified as cyberterrorism. Carefully surmising the analysis above, I would argue that cyberterrorism should be defined according to some of the following basic requirements: motivation; intention; and harm. This implies that only the cyber terrorist activities which have a terrorism intention and cause serious harmful consequences could be qualified as cyberterrorism. In addition, in this thesis, I mainly focus on critically examining how China and E&W apply their existing anti-terrorism legislation to combat ancillary cyberterrorist activities.

It is generally accepted that anti-terrorism laws should be limited to attacks that cause serious harm to persons or property. However, it is becoming more and more common among scholars to believe that ‘the anti-terrorism law should not only deal with core mischief, but also deal with the organization and finances that generate and maintain the core mischief.’ Consequently, Walker adopted a broad definition, which means ancillary cyber-activities should also fall under cyberterrorism. He claimed that this does not mean applying a strict definition is wrong, but rather that the broader perspective provides a short-hand for the full range of legal concerns and legal

---

responses.\textsuperscript{127} Similarly, in order to comprehensively compare the legal responses to cyberterrorism of China and E&W, a broad definition of cyberterrorism will be adopted in this study. Therefore, for this study, cyberterrorism not only includes cyberattacks, but also includes various activities using the Internet to sustain and further terrorism. This wider ambit coincides with the preventive strategies of China and E&W — various offences that assist terrorism are also dealt with by anti-terrorism laws.

\textbf{2.3 Literature Review of the Relationship between a Legal System and Cyberterrorism}

In order to explore whether the relationship between the legal system and the legal response to cyberterrorism in China and E&W is necessary or contingent, it is necessary to conduct a literature review of existing work to have explored the relationship between regime type and the responses to terrorism.

\textbf{2.3.1 The Relationship between a Legal System and the Legal Response}

Some of the literature has argued that a legal system frames the jurisdiction’s legal response to terrorism, and this claim will be elaborated upon below. However, most have focused on the common law system or Commonwealth countries and the legal responses to terrorism in these states. China’s legal responses to cyberterrorism have meanwhile been afforded scarce attention, with the relationship between legal systems and legal responses to cyberterrorism in the contexts of China and E&W even less studied.

Kent Roach argued that constitutional norms, local conditions, geo-historical factors and culture are significant driving forces behind divergence in counter-terrorism law in different jurisdictions. For example, many Commonwealth states (e.g. Canada and Australia) refer to the UK’s anti-terrorism laws when defining terrorism, but they are each affected by their own historical and constitutional norms. This demonstrates the

way in which legal, political and social conditions shape the definition of terrorism in different jurisdictions. Through comparative case studies of political structure and culture, as well as through examining the differences in the evolution of anti-terrorism policies in Canada and the UK, Daniel argued that the domestic political structure, legal system, human rights culture and geopolitics all influence the evolution of anti-terrorism measures. In addition, Lu Hong et al. did a quantitative research on comparative analysis of cybercrimes and legal enforcement in China and the US and emphasized the divergences of law enforcement in both nations. But this research did not critically examine the law enforcement within legal principles in both nations, and did not go further to explore the relationship between legal systems and legal responses to cybercrime in China and the US. Furthermore, they argued that “the divergence of law enforcement in both countries indicates how one nation’s specific practice is essentially rooted in its unique context.” Similarly, through critically examining China’s anti-terrorism politics and legal approaches, the authoritarian features of China’s anti-terrorism policy are revealed. Therefore, it could be concluded that China’s political and legal system does indeed frame its anti-terrorism approaches.

It should be noted that even if laws are identical, when they are transplanted into other jurisdictions with a different legal, political and social environment then there may be different effects. For example, Malaysia, Singapore, Ethiopia and Pakistan, by borrowing the UK’s TA2000, may bring their judiciaries and societies cumbersome challenges courtesy of overbroad terrorism laws. Moreover, Roach also expressed concern that countries that abuse terrorism laws may seek to legalise their counter-terrorism approaches by drawing on the anti-terrorism laws of the UK or other democratic countries.

---

130 Ibid 134.
133 K Roach, ‘Comparative Counter Terrorism Law Comes of Age’ in K Roach(ed), Comparative
Some work has focused on a comparative analysis of legal responses to terrorism in common law jurisdictions (such as the UK, the USA and Canada), in which a lot of similarities could be observed, such as the vague and broad definition of terrorism, extensive legislation criminalising terrorism, a tendency to rely on existing criminal laws to combat terrorism, the expansion of investigative powers, the extension of detention of suspected terrorists without charge, the criminalisation of new offences and increasingly harsh sentences.134 By analysing terrorism cases, it is concluded that the legal principles of the major common law jurisdictions are similar when dealing with this trans-national problem.135

However, even though the liberal democratic jurisdictions have similar systems, there are still some differences in their legal responses to terrorism. By examining legal definitions of terrorism in four Commonwealth nations (the UK, Australia, Canada, and New Zealand), Hardy and Walliams found that despite their definitions of terrorism sharing some similarities (such as wording and structure), there were a number of significant differences in how these four countries had defined terrorism. 136 Exploring these differences leads us to broader questions about how cyberterrorism should be defined, both in legislation and political discourse.137

2.3.2 Regime Types and Effectiveness of Combating Cyberterrorism

Compared with authoritarian states, democracies are more likely to be the targets of both conventional terrorism and cyberterrorism.138 The rationale underpinning this...
assumption is that democracies are more likely to respect the privacy of individuals thus making terrorist activity more accessible, while authoritarian states impose a high level of cyber security through heavy surveillance and censorship at the cost of personal liberty. For example, China's censorship of the Internet is widely considered very harsh, and dominates almost all topics such as politics, military, religion and terrorism, to the point there is almost no political criticism and terrorism-related content on the Internet in China. Their contrasting focus on security and freedom is the key to distinguishing between democratic and authoritarian regimes. Democracies are inherently more concerned about personal freedom, while authoritarian countries are more likely to try to establish a solid and reliable security system to ensure the survival of the regime. China and E&W are two typical examples of these opposing approaches. The treatment of security and freedom affects policies, leadership and legal approaches to cyberterrorism.

According to some empirical research, there is a generally positive correlation between the level of freedom afforded and the number/frequency of terrorist incidents. This illustrates that the relationship between regime type and terrorism occurrence is necessary. Piazza's comparative study concluded that authoritarian states are more adept at suppressing and preventing terrorism than democratic countries. However, his research did not analyse the reasons for this being the case or what aspects of each regime type encourage or prohibit terrorism.

Schmid summarised some obstacles that democratic regimes face in dealing. These included the trade-off between civil liberties and state security being difficult for the public to accept, which may hinder intelligence collection. In addition, legal

---


Symposium on Security and Privacy
restrictions make it necessary for democratic regimes to prosecute terrorists in accordance with the due process. In contrast, authoritarian governments are less constrained and in some cases not at all constrained by these democratic values. Some scholars claimed that non-democracies’ lack of legal norms and complicated institutions make their counter-terrorism measures relatively effective.

2.4 Literature Review of Critical Analyses of Legal Responses to Cyberterrorism

In order to conduct a comprehensive comparative analysis of the legal responses to cyberterrorism in China and E&W, it is necessary to review the existing work to have critically examined the use of existing anti-terrorism laws to deal with cyberterrorism in both jurisdictions.

(1) E&W

A prominent theme in contemporary scholarship is the exploration of the legal responses to cyberterrorism at international and domestic levels. Scholars in the Cyberterrorism Project explored the concept of cyberterrorism, assessed the threat posed by it and considered what would constitute an appropriate response to it. Meanwhile, Mott adopted the “Critical Terrorism Studies (CTS)” approach to examine the discourse about the threat to the UK posed by cyberterrorism.

---

150 CTS is a sub-discipline of Terrorism Studies, which aims to solve significant analytical and normative limitations in Traditional Terrorism Studies literature.
Elsewhere, some scholars have criticised traditional terrorism studies for their alleged limitations with regard to definitional matters. Pertinently, cyberterrorism has inherited the same definitional dilemma. Supporters of CTS claim that governments, including the UK government, have misused the label of terrorism, in which legitimate forms of resistance, insurgency or civil conflict are inappropriately referred to as terrorist groups or incidents. Such mislabeling may lead a government to abuse its power and legalise extreme measures. For example, in E&W, detention without charge was extended up to 28 days under the Terrorism Act 2006 (TA 2006), s 41.

The current legal approaches to cyberterrorism in E&W have been the subject of much criticism, mainly focusing on the tension between the imperative of prevention and early intervention and the impact on human rights and the rule of law of introducing excessively broad and vague criminal offences. Some criminal law theorists have expressed concern that expanding the application of existing criminal law and facilitating early intervention to increase security against terrorism might lead to the unjustifiable sacrifice of rule of law values and human rights. Lord Carlile QC and Stuart Macdonald argued that criminal law has both preventive and punitive functions, and that it is necessary to create precursor offences due to the limitations of the inchoate offences of attempt, conspiracy and encouraging crime. Furthermore, they advocated the use of the principle of normative involvement to both justify the extension of criminal law and to evaluate whether such precursor offences amounted to overreach.

---

153 It has been said that there are more than 100 definitions offered for terrorism, G Weimann, ‘Cyberterrorism: The Sum of All Fears?’ (2005) 28(2)SCT 129, 129-149.
154 V Erlenbusch, ‘How (not) to Study Terrorism’ (2014) 14(4) CRISPP 470, 470-491.
158 Ibid.
In addition, a number of criticisms have been levelled at the wide range of precursor offences in the UK with respect to: their often broad and ambiguous wording; possibilities of causing intrusive and discriminatory investigations; the severity of aggravated punishments for terrorism; the overlap and necessity of these offences; and the lack of empirical work to support the preventive effect of introducing these offences. Similarly, Clive Walker examined the existing legislations in the UK to deal with hostile cyberattacks and ancillary cyber activities, and argued that ‘sweeping legislation has the distinct disadvantages not only of being unproductive but also of giving a signal of undue alarm and potentially criminalizing political rather than the violent.’ He also proposed that any legal initiative to react to cyberterrorism should adhere to the following legal principles: ‘rights audit, democratic accountability, constitutionalism’.

Much of the literature has focused on the expand the boundaries of criminal law by enacting new inchoate offences to prevent terrorism. Some rationale underpinning the preventive terrorism offences has been offered in some of the academic work. Firstly, after 9/11, the international response to terrorism seems to have been more prone to prevention and pre-emption, which has been reflected in the forward-looking


161 It means that the rights of individuals are respected according to traditions of the domestic jurisdictions and the demands of international law. Ibid, 626.

162 Ibid.

preventive counter-terrorism legislation promulgated in both China and E&W. Secondly, although the specific anti-terrorism legislation in China and E&W is not the same, there are some common characteristics of prevention and a focus on ensuring public safety and protection from terrorist threats. It is accepted that prevention is a legitimate goal of criminal law, based on a state’s duty to prevent harm. It is also acknowledged that one of a state’s fundamental duties is to ensure public safety and security, and to protect the public from harm. Furthermore, compared with other controversial preventive measures (such as TPIMs and control orders, and indefinite detention), it is often argued that prosecution is the preferred way to fight terrorism, by applying the so-called “priority of prosecution” approach.

However, Stuart et al asserted that ‘the potential self-defeating nature of these precursor offences should be taken into account, which may undermines both the rationale for prosecution as the measure of first resort and the moral authority and legitimacy of the criminal law.’ This means that offences are overbroad, unclear and vague, which may penalise innocent acts, undermine basic criminal law principles and

---

166 A Ashworth and L Zedner, ‘Just Prevention: Preventive Rationales and the Limits of the Criminal Law’ in RA Duff and SP Green (eds), Philosophical Foundations of the Criminal (OUP 2011) 281 and See Chapter 2 for further explanation on the importance of prevention in decisions on criminalization; for a discuss of the state’s duty to prevent harm and the right to security, see A Ashworth and L Zedner, Preventive Justice (OUP 2014) ch 1; L Lazarus, ‘Positive Obligations and Criminal Justice: Duties to Protect or Coerce?’ in JV Roberts and L Zedner (eds), Principled Approaches to Criminal Law and Criminal Justice: Essays in Honour of Professor Andrew Ashworth (OUP 2012); L Lazarus, ‘the Right to Security’ in R Cruft, M Liao and M Renzo (eds), The Philosophical Foundations of Human Rights (OUP 2014).
167 Details could be found in Chapter 7.
erode civil liberties in the pursuit of security. In addition, criminalisation of a wide range of precursor offences and early intervention may capture innocent and harmless acts, which may violate principles of proportionality, certainty, minimal criminalisation.170 Furthermore, Lord Carlile QC and Stuart Macdonald distinguished cyber terrorism from cyber preparatory acts. They considered that if such online preparatory activities were to fall under the substantive actions of cyber terrorism, then the powers and procedures related to terrorism would also expand dramatically. Allowing these terrorism-related powers and procedures to be applied remotely from terrorism attacks may result in damage to the rule of law and human rights. They therefore argued that the statutory definition of cyberterrorism should be narrowly defined to limit the scope of special powers and procedures related to terrorism.171

After critically examining the introduction of offences to extend inchoate liability, Simon argued that they cannot be justified according to a framework of principles based on respect for autonomy, liberty and fundamental human rights.172 In addition, there is a consensus among many scholars that there is insufficient evidence to prove that counter-terrorism measures are effective in preventing terrorism and that in some cases harsher laws and penalties may actually be counterproductive.173

Many scholars have argued that expanding the boundaries of criminal liability in the UK goes too far in pursuit of the aim of prevention. Therefore, they proposed that legislative restrictions should be imposed on anti-terrorism powers.174 For example,

174 A Ashworth and L Zedner, Preventive Justice (Oxford University Press 2014); P Ramsay,
as many scholars have suggested, this stratum of precursor offences is necessary, but their boundaries should be carefully justified and circumscribed.\textsuperscript{175} Mill considered what restrictions should be given to preventive power implemented by a State.\textsuperscript{176} Meanwhile, Simon proposed a framework for limiting principles and constraints on the criminalisation of terrorism-related offences to ensure that the reach of criminal law is not extended unjustifiably in the name of prevention.\textsuperscript{177}

(2) China

 Compared with the West, China’s academic research on cyber terrorism started relatively late. The research on cyberterrorism in China has mainly drawn on some ideas and achievements from abroad, and is research on cyberterrorism is not as deep and broad as the Western equivalent. So far, most of the literature on cyberterrorism in China entails echoes descriptions provided by state organisations and/or foreign scholars. For example, the definitions, characteristics, typologies, development, threats and reasons of cyberterrorism and general countermeasures are illustrated in such research.\textsuperscript{178}

\begin{flushright}
\textsuperscript{176} JS Mill, \textit{On Liberty} (1859)165.
\end{flushright}
There is no comparative study of legal responses to cyberterrorism between China and other jurisdictions in Chinese academia. There has been no comparative study of the legal responses to cyberterrorism in China and other jurisdictions in Chinese academia. I was only able to find one article regarding a comparative study on inciting terrorism online in China and the UK. Through examining existing provisions relating to incitement to terrorism online, the researcher concluded that the Chinese legislation was still rough and the UK’s legislation served as a good reference point for China to improve its law.\textsuperscript{179} However, despite the huge differences between the legal systems of China and the UK, the researcher did not explore the impact of these on specific legislation pertaining to the incitement of terrorism. Perhaps the earliest academic study on cyberterrorism in China was a master's thesis in 2003, in which the author only described the phenomenon of cyberterrorism in general and the inducing factors, as well as providing an analysis of the likelihood of cyberterrorism incidents. However, this thesis did not critically analyse the legal responses to cyberterrorism and the distinctive characteristics of cyberterrorism in China.\textsuperscript{180}

In order to explore the topic of legal responses to cyberterrorism in both China and E&W, the CTS\textsuperscript{181} approach seems appropriate to explore this area. At present, few scholars in China use this method to study cyberterrorism, which is a shortcoming this thesis aims to address. Richard Jackson laid out four main criticisms of what he and other CTS scholars call “orthodox terrorism studies” and these are introduced below.\textsuperscript{182}

(1) There is a series of methodological and analytical shortcomings in traditional

\begin{footnotesize}


\end{footnotesize}
terrorism studies. Some of these shortcomings are particularly pertinent to the study of cyberterrorism in China. For example, over-reliance on second-hand data is also common in academic research on cyberterrorism in China. Specifically, some Chinese scholars use second-hand data to explore the characteristics and development trends of cyberterrorism. Only a few scholars work with actual first-hand research. One rare example of this was an original empirical work on cyberterrorism and legal responses based on 100 random cases, which ascertained that cyberterrorism is difficult to prevent and that the current criminal boundaries were insufficient to cover all categories of cyberterrorism, prompting the suggestion to expand the scope of criminal law and to strengthen cooperation between states and public-private organs.

In China, due to the sensitive characteristics of terrorism and cyberterrorism research topics, the primary data from anti-terrorism research centres is confidential and not open to public access. In this thesis, I did not seek to obtain confidential information regarding counter-terrorism or cyberterrorism. Instead, openly-accessible materials (e.g. provisions, cases, and policies) were used as primary data to examine China’s legislation, practice and discourse in relation to combatting cyberterrorism. Ultimately, a lack of confidential information does not constitute an obstacle to this research.

The wording and information regarding the scope of and countermeasures to cyberterrorism in the academic literature could be traced to official documents, including the following excerpt from the second symposium on combating cyberterrorism.

---

186 Yu Zhigang, Guo Zhilong, ‘Cyberterrorism Crimes and Responses from Law in China: Analysis and Reflection Based on 100 Random Cases(网络恐怖主义犯罪在中国法律应对——基于 100 个随机案例的思考)’(2015) 55(1) Journal of Henan University Social Science.
cyberterrorism under the framework of "Global Counter-Terrorism Forum" on 21 October 2016: 'China resolutely combats all forms of terrorism and is committed to strengthening international counter-terrorism cooperation' and 'all terrorist-related activities carried out through the Internet can be included in the category of cyber terrorism.'  

(2) Research into cyberterrorism is highly repetitive and scholars’ arguments tend to be very similar. For instance, many scholars have proposed that China should: create a specific anti-cyberterrorism provision to clarify the definition and scope of cyberterrorism; 189 construct an effective prevention system and a cyber surveillance system to contain the spread and radicalisation of terrorist ideology at an early stage 190; and engage in active international cooperation and information-sharing.191

(3) Jackson claimed that the close connections between anti-terrorism researchers and national institutions meant that the line between scholarship and state-linked policy research has become blurred. 192 Such criticism is highly relevant when reviewing the literature to have studied the legal responses to cyberterrorism in China. The Chinese government dominates the counter-terrorism research in China in the form of news reports, commentaries, academic conferences and research papers. 193

---

190 Zhang Jiaming, 'Legislative governance of cyber terrorism in the era of big data(大数据时代网络恐怖主义的立法治理)' (2018) 1 South China Sea Law 81-86.
193 Zhang Chi, 'How does Chinese Communist Party Legitimise its Approach to Terrorism?' (DPhil
In addition, all anti-terrorism research centres in China are affiliated with state-funded public universities. These centres have established their own database of the geographical information regarding international terrorism and it produce the Yearbook of International Terrorism and Counter-terrorism annually (2017).

The close connection between academia and the State prevents scholars in China from carrying out critical analysis that may be considered hostile by government officials, and they instead tend to replicate the state discourse on terrorism. Scholars have avoided critically exploring some key issues related to the negative impacts of counter-terrorism measures, and tend to avoid challenging anti-terrorism legislation. For example, due to their alignment with the party line, Chinese scholars seldom challenge the state definition of terrorism. The official positions of “cracking down all forms of terrorism” and “priority of national security and social stability” are often replicated in scholarly works published in China.

194 There are two official anti-terrorism research centers funded by the China’s government: The Centre for Counter-terrorism Research at Zhongnan University of Economics and Law, established in 2016, and the Counter-terrorism Research Centre at Northwest University of Political Science and Law established in 2014. The latter has its own website, Anti-terrorism Information, where it publishes terrorism-related news, research reports and commentaries.

195 For example, China Institute of Contemporary International Relations, Yearbook of International Terrorism and Counter-terrorism annually (Current Affairs Press 2017); Zhang Chi, ibid.


therefore claim that it is effective and justifiable to implement a preventive strategy, and that the criminal law should intervene at an early stage to protect collective interests. Moreover, some scholars claim that it is justifiable to expand the boundaries of terrorism-related offences.

Because of their alignment with the official position, many scholars take it for granted that criminal law will intervene in cyberterrorism activities at an early stage and that a wide range of precursor offences will be criminalised. In most of the Chinese literature, the terms “cyberterrorism” and “cyberterrorism crime” could be conflated because the Chinese researchers take it for granted that cyberterrorism is a criminal act. Some scholars are optimistic about China’s existing terrorism legislation, and believe that it is relatively complete and effective when it comes to countering cyberterrorism, having learned from other countries’ experiences. However, they rarely question whether it is in accordance with the basic principles of criminal law and whether it undermines individual human rights protection.

(4) China’s legal approaches to terrorism represent a good example of Robert Cox’s

Practitioners”, Zhuhai, December 2017) 565-578.


“problem solving theory.” This theory asserts that ‘they take the situation as they find it,’ leading the established relationships and institutions to work smoothly by offering specific suggestions on how to deal with “terrorism” without considering the negative impacts on the rule of law. Most Chinese scholars positively support the extension of the scope of criminal law and cracking down on the terrorist acts. For example, Pi Yong argued that indirect incitement of terrorism (such as glorification, denial or defence of terrorism) should be criminalised. Furthermore, Wang and Liu claimed that the criminal law should intervene at an early stage because terrorists use cyber space as a tool or target to exert influence on the real world, such as by making threats, intimidating governments and creating an atmosphere of social panic, which are all equivalent to the dangers of violent terrorist activities. Shu and Wang went further by arguing that browsing or illegally accessing terrorism-related information should also be criminalised, and that it was necessary to pre-emptively punish offenders without sufficient proof in order to protect society.

Self-alignment and self-censorship limits Chinese academic criticism of existing legal responses to cyberterrorism. Most Chinese scholars function to justify China’s counter-terrorism policies and legal responses, rather than critically challenging the existing authority and problems. Accordingly, their studies serve to reinforce the existing anti-terrorism strategy. In doing so, academic discourse echoes the official discourse (e.g. prioritisation of safety, prevention and extension of criminal liability, aggravated penalties, and transplanting Western experiences), thereby ignoring the negative impacts of these approaches (such as the abuse and arbitrariness of state power and violations of individual rights protection).

---


However, there are a few scholars who have been relatively critical of the legal responses to terrorism in China. Xu Guimin stated that to achieve the purpose of prevention, the State should not deliberately opt for severe punishment as this may contravene the principle of proportionality. \(^{209}\) Besides, Liu Renwen pointed out three problems relating to anti-terrorism legislation in China: first, the priority of security over liberty; second, more emphasis being placed on the coordination of state authorities rather than on restricting each other in combating and preventing terrorist activities; and, third, the authorities’ preference for internal supervision when protecting individual human rights. \(^{210}\) Elsewhere, Liu Yanhong claimed that anti-terrorism legislation should prioritise human rights protection, preventing the expansion of anti-terrorism powers from infringing upon civil liberties and the rule of law. \(^{211}\) Furthermore, Liu also asserted that overcriminalisation of terrorism-related offences, aggravated punishment for terrorism as well as vague and open-ended anti-terrorism legislation in China may violate principles of certainty, proportionality and legality. \(^{212}\) Similarly, Ni Chunle criticised the expansion of the scope of terrorism offences and the arbitrariness of anti-terrorism powers in China. \(^{213}\) Ni also expressed the view that the scope of terrorist crimes should be reasonably delineated, and that freedom and safety should be carefully balanced to ensure compliance with the principle of the rule of law. Moreover, blindly pursuing severe punishment and preventive anti-terrorism legislation will produce a counterproductive effect and damage the individual freedom of citizens.

He Ronggong recognised the legitimacy of China’s preventive anti-terrorism criminal legislation, but has been vigilant against further expansion of the criminal law and advocates the striking of a balance between safety and freedom. \(^{214}\) Guo and Chen


\(^{212}\) Ibid.

\(^{213}\) Ni Chunle, Special Procedures for Terrorism Crimes (恐怖主义犯罪特别诉讼程序) (Masses Publishing 2013) 5-6,45.

also considered that expanding the powers of intelligence agencies and special investigative methods should also entail balancing human rights protection.\textsuperscript{215} Wu Shenkuo has, meanwhile, asserted that the expansion of criminal law in the name of anti-terrorism does not amount to autocracy, and conforms to the rule of law, the principle of proportionality and the principle of minimum criminalisation.\textsuperscript{216}

So far, I have not found any academic research on the legal responses to cyberterrorism of the jurisdictions of China and E&W jurisdictions. Therefore, this thesis tries to fill this gap by carrying out a broader study into how authoritarian and democratic regimes respond to cyberterrorism. With respect to counter-cyberterrorism approaches, this thesis demonstrates similarities and differences between China and liberal democracies.

\textbf{2.5 Conclusion}

In the literature review presented above, none of the studies focused specifically on exploring the relationship between a legal system and legal responses to cyberterrorism in China and E&W through a comparative analysis. Under this situation, it is clear that there is a gap to be filled in order to figure out whether a state’s legal responses to cyberterrorism are contingent on the nature of that state’s legal system or not. This question will be addressed and discussed in the following chapters.


Chapter 3 Methodology

3.1 Introduction

Given that the purpose of this thesis is to critically analyse and evaluate the respective anti-cyberterrorism legal approaches in China and E&W, and then explore the relationship between a legal system and legal responses to cyberterrorism, so this study adopts a combination of doctrinal methodology, comparative methodology and socio-legal methodology.

Firstly, this chapter starts by introducing the doctrinal methodology, which aims to describe the details of existing legal responses to cyberterrorism and how these fit into the respective legal systems of China and E&W. Doctrinal methodology is employed to examine the anti-cyberterrorism-related laws, court decisions and other scholarly or NGO evaluations and analyses of related laws and cases. This part also sets out the foundations for subsequent comparative analysis.

Secondly, this chapter elaborates upon the comparative law methodology and how a comparative method is applied to achieve the research objectives. The first step of comparative legal research is to choose, establish and define what is to be compared. The subjects of comparison in this thesis are outlined in chapters 4-7, in which the relevant distinctive characteristics of legal systems are described and the legal responses to cyberterrorism in China and E&W are critically examined. Thereafter, the identification and explanatory stages are presented chapters eight and nine, which reveal the convergences and divergences in the legal responses to cyberterrorism in China and E&W, and place them within the context of entire legal systems.

I also explain the following reasons why the comparative legal method has been used in this research: (1) the common threat of cyberterrorism represents a significant stimulus for such comparison; (2) the Chinese legal system and legal responses to cyberterrorism are my “home law” and the E&W’s legal system and legal responses to cyberterrorism are my linguistically accessible law; (3) the significantly different legal systems and regime types of the chosen jurisdictions allow for a fruitful exploration into
the relationship between a legal system and legal responses; (4) comparative law seems to an effective means of researching the trans-national issue of cyberterrorism; and (5) the comparative legal method helps to better understand legal systems and anti-cyberterrorism laws in both China and E&W.

In addition, I put forward my explanation on why I compare China with E&W rather than the US, for example, as another superpower with significant influence in international debates over the (failure) of international co-operation in responding to genuinely global problems, like cyberterrorism, that traverse different jurisdictions.

Firstly, E&W has the unwritten constitution, which has an analytically significant and useful quality of rule of law in this jurisdiction, as this can provide the executive branch of government with greater latitude in developing legal responses to cyberterrorism which are disproportionate, overcriminalization, can be arbitrary and so forth. As the “rule by law” country, China also produces these same problems in dealing with cyberterrorism. Hence it is these standing conditions of the rule of law in E&W which in part explain the convergence in legal responses to cyber terrorism in China and E&W.

Another advantage of posing the question of whether the unwritten constitution of E&W provides a greater liability for disproportionate and arbitrary legal responses is that it opens up an interesting point for further research in this area: are written constitutions any better at constraining arbitrary and disproportionate legal responses to vaguely defined offences?

Furthermore, this thesis puts forward a hypothesis that because the autocratic regimes have less restrictions on administrative power, protects national security and collective interests, thereby ignores individual rights, so its legal response to cyberterrorism is fundamentally different from that of democratic countries that restrict state power to protect individual rights. By contrast, the nature of democratic regime involves a balance between security and respect of personal liberties. These contrasting emphases on security and liberty are the key factors to distinguish between democracies and authoritarian regimes. According to Rutland, “democratic states are
inherently more concerned with individual liberties while authoritarian states are far more likely to try to construct a firm and reliable security system to ensure the survival of their regime".\textsuperscript{217} So China and E&W are both good examples of these contrasting viewpoints. Understanding how these priorities and viewpoints affect political and legal systems is incredibly important to understanding their legal approaches to combat cyberterrorism. Therefore, different regime types in China and E&W may cause fundamental differences in the legal response to cyber terrorism in the two jurisdictions.

Thirdly, this chapter sets forth the socio-legal methodology for investigate whether the substantive relationship between a legal system and legal responses to cyberterrorism is contingent rather than necessary.

### 3.2 Doctrinal Methodology

The doctrinal methodology (black-letter approach)\textsuperscript{218} aims to describe legal rules and principles in detail, and this represents the starting point for the subsequent comparative legal analysis. Accordingly, the doctrinal method is employed in this thesis to ascertain the precise status of the existing law.\textsuperscript{219}

Problems ordinarily solved in comparative legal research include: ‘what do we intend to compare?’; ‘why have we chosen a comparative project?; and, perhaps most importantly, ‘what methodology do we intend to use?’\textsuperscript{220} To answer the first of these three questions, this thesis compares and contrasts the legal systems and legal responses to cyberterrorism in China and E&W.

Roach stated that: ‘one of the great challenges of studying counter-terrorism laws is that they cross traditional disciplinary boundaries within academia and even within


\textsuperscript{218} T Hutchison and N Duncan, ‘Defining and Describing What We Do: Doctrinal Legal Research’ (2012) 17(1) DLR 83, 83-119.

\textsuperscript{219} I Dobinson and F Johns, ‘Qualitative Legal Research’ in M McConville and Wing Hong Chui(eds), Research Methods for Law (Edinburgh University Press 2007) 19: arguing that ‘the doctrinal research methodology is concerned with ‘ascertaining the precise state of the law on a particular point’.

law...221 Within this outlook in mind, the doctrinal methodology runs through this entire thesis, which also provides a comprehensive comparative analysis of how China and E&W apply their existing anti-terrorism laws to combat cyberterrorism. In this thesis, the main materials for doctrinal research in China and E&W are: (1) anti-cyberterrorism-related legislations; (2) official government reports; (3) cyberterrorism-related cases (eg. China Judgement Online at the Supreme Court of China222); (4) NGOs' studies (especially those of Human Rights Watch and Amnesty International); (5) academic literature; (6) online resources from Google Scholar, HeinOnline, Westlaw, Lexis Nexis and CNKI223, among others; and (7) news reports or publications.

In almost all legal studies, it is necessary to conduct some doctrinal research to lay the foundations for subsequent critical analysis.224 Pertinently, the purpose of doctrinal analysis is to explore the development of legal principles and how the law works in a specific context.225 As such, chapters four and six provide a predominantly doctrinal analyses of the distinctive characteristics of legal and political systems, and basic criminal law principles in China and E&W, in order to set out the relevant critically examination of legal responses to cyberterrorism in both jurisdictions. Furthermore, the anti-terrorism laws in China and E&W are constantly revised or changed, so the doctrinal approach produces expositions of new or different aspects of a legal doctrine.226

3.3 Comparative Methodology

Applying the black-letter approach alone is not sufficient because it does not allow for

---

222 In July 2013, the "China Judgments Online" (http://wenshu.court.gov.cn) developed by the China's Supreme People's Court (SPC) officially went online.
223 China Academic Journals full-text database (also known as CNKI) is the largest and continuously updated Chinese journals database in the world.
224 See generally T Hutchinson, 'Doctrinal Research: Researching the Jury' in D Watkins and M Burton (eds), Research Methods in Law (Routledge 2013). Hutchinson argues that 'the doctrinal method still necessarily forms the basis for most, if not all, legal research projects' (at 7) and that doctrinal research 'constitutes the foundation or starting point of most legal research projects' (at 28).
226 Each time an amendment is made, the researcher is required to interpret the law on the basis that it forms a system of interrelated-rules. M Salter and J Mason, Writing Law Dissertations: An Introduction and Guide to the Conduct of Legal Research (Pearson Education Limited 2007) 189
the topic to be explored from a broad enough perspective. Meanwhile, comparative legal methodology is particularly valuable when analysing the same trans-national issue of cyberterrorism in China and E&W, especially as the process of globalisation continues to prevail. Eberle contended,

> In our increasingly globally linked world, comparative law needs to take an ever more crucial role. With the rise of important new developments over the last thirty years, like the proliferation of the computer and the internet, we are linked in important common ways. The computer, and especially its generation of the internet has made us, in effect, a global village.

With regard to this aspect, Razak contended that comparative research ‘stimulates awareness of the cultural and social characters of the law and provides a unique understanding of the way law develops and works in different cultures.’ Meanwhile, Eberle added that ‘applied to law, the act of comparison provides insight into another country’s law, our own law, and, just as importantly, our own perceptions and intuitions—a self-reflection that can often yield insight into our view of the law.’ With this in mind, the comparative method is expected to allow for a better understanding of existing anti-cyberterrorism legislation in China and E&W.

David Nelken noted that, ‘Comparative work is both about discovering surprising differences and unexpected similarities.’ Furthermore, he also argues that, “it is necessary to apply theoretical justifications to explain why such findings are so interesting (because unexpected).” In this thesis, by comparing the existing anti-cyberterrorism laws in China and the E&W, there are, not surprisingly, many differences, but further examination also reveals some similarities, perhaps more than most would have assumed.

---

232 ibid 31.
3.3.1 Cultural Comparative Methodology

There are various purposes that comparative methodology can serve, and various approaches to understanding the benefits and drawbacks of comparativism. For example, the universalist view of comparative law is as a functional science. Universalists view such law ‘as an autonomous system, whose form and content are ultimately similar in all cultures’, and consider that it has little to do with local culture and social background. Universalists claim that analysis of cultural contexts is theoretically incoherent and lacking in rigour because it lacks a certain degree of scientificity and cannot be empirically quantified.

However, the cultural comparativist view which transcends the comparison of rules and takes into account the social, political and cultural backgrounds of different jurisdictions to shape the law. Since the research focus of this thesis is to explore the relationship between legal systems and the legal responses to cyberterrorism in China and E&W, for the purposes of this thesis, cultural comparativism is most relevant and helpful.

Cultural comparativists(such as Liora Lazarus, Pierre Legrand, and David Nelken) are sceptical of universalist views, arguing that comparative studies cannot only focus on legal rules, because ‘they forget about the historical, social, economic, political, cultural, and psychological context which has made that rule or proposition what it is’. The purpose of their comparative research is to explore how the social, political and cultural contexts of different jurisdictions shape legal rules. This thesis will compare the contexts of the given legal systems and legal responses to cyberterrorism in both

---


236 R Cotterell, ‘The Concept of Legal Culture’ in D Nelken(ed), *Comparing Legal Cultures: Socio-legal studies series* (Dartmouth1997) 13-14

237 Represented in the works of authors such as Liora Lazarus, Pierre Legrand, and David Nelken, referred to as ‘Cultural comparativists’, discussed below.


jurisdictions in order to explore whether legal systems shape legal responses.

John Merryman admitted that there were instances in which rule-comparison could be directly useful, but also argued that ‘scholarship is supposed to have larger concerns’ and, as such, it is crucial to understand the ‘context or institutional setting in which rules operate’. Therefore, a purely doctrinal comparative legal study which only focuses on the legal rules of different jurisdictions may overlook the differences in terms of legal, political and cultural background. If these differences affect the development of anti-terrorism laws, the universalist view will indeed inevitably ignore this key point. Therefore, in order to more comprehensively explore whether a legal system shapes the legal response, it is not enough to purely compare the anti-cyberterrorism laws in China and E&W, as the legal systems they operate within should also be compared.

Comparative legal research can help to understand how foreign legal systems work, as well as provide for a better understanding of the laws and culture of the author’s own country. Nelken’s point about embracing a general world view closer to the foreign place where the insider-outsider is located may have greater salience in the context of a researcher who is living in a country that has a significantly different culture from that of their own. As the political, cultural and legal systems of China and E&W are completely different, comparing their legal responses to cyberterrorism may have unexpected and creative results. As the following chapters shown, there are, unsurprisingly, a number of divergences in the legal responses to cyberterrorism in China and E&W due to their different legal systems however, their legal responses, unexpectedly, have more in common with each other.

3.3.2 Comparability

244 D Nelken, Comparative Criminal Justice (SAGE Publications 2010) 99.
A commonly cited norm of comparative law methodology is that 'like must be compared with like.' This, at first sight, would seem to make the China and E&W's cyberterrorism legal responses incomparable because of their different legal and political systems. However, different legal systems does not preclude comparative research. In fact, there is no unified standard methodology in comparative law - the possibility of comparison 'depends on the existence and availability of data' and the purpose of comparison. Dannemann noted, 'there is no point in comparing what is identical, and little point in comparing what has nothing in common.' The scope of comparative law research is therefore wide, and can be carried out within the same legal family (such as common law and civil law) or between different legal families. Comparative research is used to explore how different legal systems and legal cultures solve common problems in different ways. Therefore, in this research, I try to critically compare how China and E&W use their existing anti-terrorism laws to combat cyberterrorism in different and similar ways. However, upon further analysis, what is unexpected is that there are many similarities in the anti-terrorism legislation, practices and policies in dealing with cyberterrorism in China and E&W.

In addition, the "comparability" could be discussed in relation to both macro and micro dimensions. At the macro level, comparative scholars claims that "comparability" is related to the purpose of comparison, which determines the choice of the legal systems to be compared. Accordingly, comparative research is not limited to legal systems that are similar or shared broadly common attributes. In this thesis, the research aim is to explore the relationship between a legal system and legal responses, so two quite different legal systems have been chosen. At the level of micro-comparison, it is generally believed that the basis of comparison is "functional comparability", whereby law is a response to human needs, so all rules and systems are designed to meet

---

247 Ibid 49.
248 G Dannemann, ‘Comparative Law: Study of Similarities or Differences?’ in M Reimann and R Zimmerman (eds), The Oxford Handbook of Comparative Law (OUP 2006) 384.
249 C Morris and C Murphy, Getting a PhD in Law (Hart Publishing 2011) 37.
250 Ibid 183.
252 Ibid 561.
these needs.\textsuperscript{253}

3.3.3 The Four Reasons Behind Using the Comparative Legal Method?

(1) The comparative law method is an effective means of achieving the research aim, which is to undertake a comparison of legal approaches to counter cyberterrorism in China and E&W and then figure out whether the relationship between a legal system and legal responses to cyberterrorism is contingent or necessary. In order to adhere closely to the purpose of the research, I have chosen one jurisdiction representative of democracy (E&W), and another jurisdiction representative of non-democracy or autocracy (China).

This thesis puts forward a hypothesis that because the autocratic regimes have less restrictions on administrative power, protects national security and collective interests, thereby ignores individual rights, so its legal response to cyber terrorism is fundamentally different from that of democratic countries that restrict state power to protect individual rights. Therefore, different regime types in China and E&W may cause fundamental differences in the legal response to cyber terrorism in the two jurisdictions. In this thesis, in order to analyze the impact of the different types of regimes represented by China and E&W on the legal responses to cyberterrorism and the relationship between the legal system and the legal responses, it is necessary to first define a clear definition for each type.

Dahl argued that representative democracy allows citizens to freely and fairly elect the executive and legislative bodies, citizens freely exercise their right to vote and compete for public office, as well as system guarantees for freedom of association and speech (e.g. an independent judiciary, the absence of censorship).\textsuperscript{254} On the contrary, authoritarian systems do not allow open and competitive elections, and often “it is related to the existence of a single leader or small ruling group, weak political


mobilization and legal restrictions on pluralism”. Quan Li adopted the minimalist definition of democracy, which means that if the opposition party or other parties have a chance to win and take office through public elections, the country is classified as a democratic country; otherwise, the country is regarded as an authoritarian country. According to David Beetham, the definition of democracy could be characterized by popular control and political equality, which means citizens fairly and openly participate in elections, and all electors’ votes hold the same weight, and the same rights run for the office, express their opinions equally. In essence, representative democracy requires the people to indirectly control the government by controlling who makes decisions in the government.

Furthermore, Juan Linz defines the authoritarian regime type as a political system “with limited, not responsible, political pluralism without elaborate and guiding ideology, but with distinctive mentalities, without extensive nor intensive political mobilization, except at some points in their development, and in which a leader or occasionally a small group exercises power within formally ill-defined limits but actually quite predictable ones.”

According to this definition, authoritarian regimes usually do not elect new leaders publicly, but are passed on to their children or political allies by previous leaders as a form of inheritance. The characteristic of authoritarian regimes is that few referendums participate in elections, and even if they do, these votes are meaningless. In addition, the authoritarian regime is controlled by a single person or group with the power to make decisions for the state, and the boundaries of power are not clear. Authoritarian regimes do not pay much attention to the protection of individual rights such as freedom of speech and thought, but are committed to building a highly secure and protected society. Rutland define an authoritarian regime as “any regime that is

---

257 Q Li, ‘Democracy, Autocracy, and Expropriation of Foreign Direct Investment’ (2009) 42(8) CPS 1098, 1102.
tightly secured, controlled by one person, party, or small group that maintains this
control without the use of elections, or with the use of limited elections, and that holds
decision making power for the state”. 262

In light of this, China and E&W have quite different regime types and also have
significant differences in terms of their legal, cultural, and political attributes, which
have important implications on their choice of different approaches and laws to deal
with cyber terrorism.

Meanwhile, both jurisdictions share a common desire to combat cyberterrorism
effectively and legitimately. Through comparative legal methodology, a number of
similarities and differences in the legal responses to cyberterrorism in China and E&W
could be found. On the one hand, such convergence indicates that China and E&W
are facing similar problems when coping with cyberterrorism; on the other hand, the
divergence indicates how each jurisdiction’s legal approach is essentially rooted in its
unique context.263

(2) Linguistically accessibility is an essential element of making this comparative study
feasible and meaningful. A number of researchers have compared common law
systems that mainly use the researcher’s own language.264 However, as globalisation
prevails, both legislation and research are written in different languages and countries.
When choosing which legal systems to be included in the comparison, the researcher
often simply chooses their ‘home law’, and the law of another country which is
linguistically accessible and with which the researcher may have some personal
ties.265 In the case of my research, the Chinese legal system and legal responses to
cyberterrorism fall under my “home law” while E&W’s legal system and legal responses
are my linguistically accessible and also where my current PhD university is located. I
compare the two legal systems and legal responses in their two official languages, with
the aim of gaining an accurate understanding and background of the legislation and

262 Ibid.
263 H Lu, B Liang and M Taylor, ‘A Comparative Analysis of Cybercrimes and Governmental Law
265 G Danneman, ‘Comparative Law: Study of Similarities or Differences?’ in M Reimann and R
(3) The common threat of cyberterrorism is a significant stimulus for this comparison and exploration of the relationship between a legal system and legal responses. Similarity of problems is essential for a comparative study, which arouses great interest from the legislature, courts or advisers as to how other legal systems solve the same problem.\textsuperscript{266} Geoffrey Wilson also stated that the study of comparative law enables representative countries of different legal systems and their scholars and practitioners to participate in solving the same problem.\textsuperscript{267} Since cyberterrorism is a global and trans-national problem, it is not sufficient to rely solely on the domestic legal approach to combat cyberterrorism, as it is necessary to look at other countries’ legal responses as well. Comparative law seems to be an effective means of researching this trans-national issue, which is applied by numerous academic scholars and legal practitioners.\textsuperscript{268} With the increase in cross-border activities and the increasing effect of widespread political movements, there is a growing need to compare of legal systems from different jurisdictions.\textsuperscript{269} Additionally, according to Zweigert and Kötz: ‘the method of comparative law dissolves unconsidered national prejudices, and helps us fathom the different societies and cultures of the world and to further international understanding.’\textsuperscript{270} Moreover, both China and E&W do not have specific anti-cyberterrorism legislation, and rather apply their existing counter-terrorism laws to deal with the issue. Therefore, their legal responses may give rise to a number of problems such as over-criminalisation, unpredictability, lack of counterbalance, violation of proportionality, ill-defined, arbitrariness, and expansion of executive powers. The similarities and differences in China and E&W’s handling of this same issue have been interesting.\textsuperscript{271}

While the social, cultural and political conditions that inform legal practices in China are markedly different from those of Western jurisdictions, I nevertheless believe that

\textsuperscript{266} ibid 17.
\textsuperscript{267} M McConville and WH Chui (eds), \textit{Research Methods for Law} (Edinburgh University Press 2007) 88.
\textsuperscript{268} Details could be found in Literature Review Chapter 3.
\textsuperscript{269} See OG Chase, ‘Legal Processes and National Culture’ (1997) 5 CJICL 1.
\textsuperscript{270} K Zweigert and H Kötz, \textit{An Introduction to Comparative Law} (3rd edn, Oxford University Press 1998)15-16.
\textsuperscript{271} The details of such similarities and differences can be found in Chapter 8.
comparative criminal law studies, when attuned to ‘difference’ and placing the ‘law in context,’ can shed new light on their respective legal systems and how they respond to common trans-national threats like cyberterrorism.\(^{272}\) David Nelken claimed that, in comparative criminal justice: ‘transnational crime activities [for example, Cyber terrorism] and responses to them help transform and transcend differences between units defined as nation-states.’\(^{273}\) In light of this, my research not only needs to compare the relevant cyberterrorism regulations of China and E&W, but it should also compare the legal principles and legal contexts behind them.

(4) The comparative law method provides a deeper understanding of a legal system and legal responses to cyberterrorism in China and E&W. Moreover, as mentioned above, it helps me to interpret and examine the existing legislation countering cyberterrorism in China and E&W. As Sacco has observed, a distinctive feature of comparative law is that it plays an important role in the interpretation of legal norms of various legal systems.\(^{274}\) Many distinguished comparative lawyers have insisted on the virtues of comparative law as a means of expanding knowledge generally and as a means of better understanding law.\(^{275}\)

Comparative law, as defined by Rainer, is a branch of jurisprudence which leads research into various aspects of different legal systems and compares and analyses them.\(^{276}\) Any comparative inquiry will have to describe those rules, legal institutions, theories, or even entire legal systems which are the object of said inquiry.\(^{277}\) It is regarded as a ‘systematic application of the comparative technique to law,’\(^{278}\) which involves the entirely or partial comparison of two or more than two legal systems.

---


Meanwhile, acquiring knowledge of foreign legal systems by conducting a comparison promotes a better understanding of one’s own legal system as well.\(^{279}\) Making such a comparison provides for a deeper understanding of certain features of the subject being studied, and therefore yields better knowledge of the different rules and institutions that are compared.\(^{280}\) It not only lets scholars realize that the legislations of a sole legal system is not the only solution to a common problems in the world. Furthermore, after making a comparison, researchers could gain a better understanding of other legal systems related to their subject. In other words, comparative law provides for a broader perspective of other legal systems, rather than focusing on only their successes and/or failures.\(^{281}\) As Kamba has pointed out, the knowledge gained by comparing different legal systems may help legislators to ‘fashion rules or principles of positive law.’\(^{282}\) With these views in mind, in this thesis, the comparative method can not only help to better understand the legal contexts and legal principles of China and E&W, but it can also critically evaluates the anti-cyberterrorism-related legislation of both China and E&W.

### 3.3.4 How is a Comparative Study Conducted?

Gerhard and John summarised the following steps of comparative inquiries: selection (of what will be compared); description (of the law and its context in the legal systems under consideration); and analysis.\(^{283}\) In addition, Reitz proposed nine principles for operating comparative work:

- Draw explicit comparison; concentrate on similarities and differences but in

---


\(^{281}\) RB Schlesinger, ‘The Role of the “Basic Course” in the Teaching of Foreign and Comparative law’ (1971) 19 AJCL 616, 618.


assessing the significance of the difference take into account functional equivalence; observe the distinctive characteristic of each individual legal system and also commonalities in dealing with the particular subject researched; push the analysis into broader levels of abstraction; give reasons and analyse the significance of similarities and differences; describe the normal conceptual world of the lawyers, look at all the sources and consider the gap between the law in the books and law in action; have linguistic skills and, if need be, anthropological skills in order to collect information (though a comparatist can also rely – if the two skills are lacking – on secondary literature); organize with emphasis on explicit comparison; and undertake research in the spirit of respect for the ‘other’.  

With these principles in mind, the first step is to choose, establish and define the content to be compared. Such content is outlined in chapters 4-7 in which the relevant distinctive characteristics of the legal and political systems in China and E&W are described, and the ways in which China and E&W use their existing anti-terrorism legislation and strategies to deal with the common problem of cyberterrorism are critically evaluated. Through this juxtaposition, contrasting and comparison, similarities and differences can be identified, but comparative studies should not only end with descriptions. They should move on to the explanation and confirmation of the findings. In other words, comparison as a research method cannot be completed by merely identifying differences and similarities, but must go further and seek to explain them. Accordingly, the next step is to explore why these similarities and differences exist between China and E&W, and what factors affect them.

The identification and explanatory stage follows, where the similarities and differences of the content being compared are identified, and placed within the context of the entire legal system. This is dealt with in detail in chapter eight, which identifies the convergences and divergences in the legal responses to cyberterrorism in China and E&W, and places them in the context of their respective legal systems and political
systems in both jurisdictions. Ultimately, the conclusion is as follows: differences in the legal system do not explain the similarities in legal responses particularly to cross-jurisdictional problems for law enforcement, such as cyberterrorism.

3.3.5 Limitations of Comparative Legal Methodology

Inevitably, this research method does have some shortcomings or limitations. For example, according to Salter and Mason, the availability and accessibility of primary materials for the legal system or legislation of the countries to be compared may sometimes be restricted. 288 This is a pertinent consideration for this research. However, the primary materials of legal systems, legal principles, legislations and cases related to cyberterrorism in China and E&W can be accessed and obtained publicly on the Internet. Therefore, this limitation does not hinder this research in this way. The same scholars also considered that comparative research methods may run the risk of a thesis only providing a narrative description of the laws of the selected jurisdictions, lacking in sufficient analytical analysis. 289 In this thesis, I intend to avoid this situation through carrying out cross-references in separate chapters and two jurisdictions, as well as by critically evaluating and comparing the legal responses of the two jurisdictions.

3.4 Socio-legal Methodology

In order to analytically examine the workings of the law, it is necessary to go beyond doctrinal analysis. 290 The value of doctrinal research can be increased with the adoption of a socio-legal method. 291 Socio-legal methodology reveals discrepancies between ‘law in books’ and ‘law in action.’ 292 This approach bridges the gap between

---

290 Thomas argues “Empirically, law is a component part of the wider social and political structure, is inextricably related to it in an infinite variety of ways, and can therefore only be properly understood if studied in that context”. P Thomas, ‘Curriculum Development in Legal Studies’ (1986) 20 LT 110, 112.
292 Although it is difficult to comprehensively define ‘socio-legal’ approach to legal studies, Philip
law, and sociology and social policy. The black-letter approach elaborates upon and explains the content of legal rules, while the socio-legal approach focuses on the functions, practices and the implications of rules. This thesis aims to study whether the substantive relations of connection between a legal system and legal responses to cyberterrorism is either necessary or contingent. Accordingly, in this thesis, apart from doctrinal and comparative methodologies, I also adopt socio-legal methodology to achieve my research aim.

There is no unified definition of socio-legal research because of its highly diverse ways in which it is implemented. A socio-legal approach ‘embraces disciplines and subjects concerned with law as a social institution, with the social effects of law, legal processes, institutions and services and with the influence of social, political and economic factors on the law and legal institutions.’^293 As Salter and Mason proposed, socio-legal methodology could expand ‘the scope of legal analysis beyond law reports and statutes to include the social, economic, gender and political factors influencing the emergence and development of legal doctrine and decision-making.’^294 In short, socio-legal research is supposed to explore how the law works in a broader socio-political context.^295 This methodology will broaden the scope of this research, which considers how the law operates in a broad legal system, legal culture, political system and social structure. Therefore, this research method will help to explore how China and E&W apply existing anti-terrorism laws to combat cyberterrorism under their respective legal and political systems, and establish whether specific legal and political systems determine legal responses.

Wheeler and Thomas suggested that ‘the word “socio” in socio-legal studies means to

---

us an interface with a context within which law exists, be that a sociological, historical, economic, geographical or other context. Socio-legal methods tend to combine the ‘legal’ and ‘social’ aspects in their research. The purpose of socio-legal methodology is to examine the law, legal system, legal phenomena and the relationship between these issues and the broader social, cultural and other backgrounds. This aligns with the purpose of this thesis; in addition to identifying the similarities and differences in the legal responses to cyberterrorism between China and E&W, the use of socio-legal methods allows us to explore the relationship between these similarities and differences and the respective legal and political systems.

Cotterrell contended that a socio-legal approach can greatly enhance the value of research. Meanwhile, Gerhard put forward the view that the legal context is relevant for the proper understanding of particular rules. Most legal rules and institutions operate in a context made up of other rules, institutions and areas of law (i.e. substantive rules interact with rules of procedure). Meanwhile, Singhal and Malik asserted that,

Socio-legal research is significant because in linking the law to society, it functionalizes law, rendering it an effective instrument for the achievement of social, political and economic objectives. Socio-legal research is important for and impacts upon government policy-makers, regulators, industry representatives and other actors concerned with the administration of justice and the legal system.

However, some scholars have accused the socio-legal method of causing the research

---

297 HP Wiratraman, ‘The Challenges of Teaching Comparative Law and Socio-Legal Studies at Indonesia’s Law Schools’ (2019) 14 AJCL 229, 229–244.
301 Ibid.
302 AK Singhal and I Malik, ‘Doctrinal and Socio-legal Methods of Research: Merits and Demerits’ (2012) 2(7) ERJ 252, 255.
to be ‘theoretical and descriptive in nature.' To prevent this research from becoming only descriptive, comparative methodology is applied alongside socio-legal methods.

According to Walker, comparative law exercises are fraught with dangers because of the explicit and sometimes subtle differences in law and practice. In addition, there are often significant differences in legal systems, power structures, politics, culture and how legal rules be interpreted and applied. Nevertheless, cross-jurisdictional comparative research which focuses on developing and testing theories that can be applied beyond a single jurisdiction, regardless of their cultural, historical or political differences. The law is seated within a culture, so it is necessary to know how it functions within the society and, more importantly, to have a more realistic look at the legal system that is being investigated.

The trans-national focus in both comparative legal research and socio-legal studies is indispensable. Vitalij proposed that the synthesis of doctrinal and socio-legal approaches within comparative legal methodology is possible when it comes to investigating the trans-national research of both ‘law in book’ and ‘law in action.’ The field of socio-legal studies is complementary to the study of comparative law. This is because the study of comparative law goes beyond just comparing legal rules, and instead compared in detail the history, theory, culture, legal system, political system and other factors behind the given rules.

The newest socio-legal approach, known as ‘law in society,’ seeks to examine ‘law in action’ and ‘how the legal system actually operates.’ As globalisation prevails, law

---

305 E Oyen, Comparative Methodology Theory and Practice in International Social Research (SAGE Publisher 1990) 1.
307 LMV Derwalt, Comparative Method; Comparing Legal Systems or Legal Culture (Speculum Juris 2006) 58.
308 A Riles, ‘Comparative Law and Socio-Legal Studies’ in M Reimann and R Zimmermann (eds), The Oxford Handbook of Comparative Law (Oxford University Press 2006) 799.
310 A Riles, ‘Comparative Law and Socio-Legal Studies’ in M Reimann and R Zimmermann (eds), The Oxford Handbook of Comparative Law (Oxford University Press 2006).
and its implementation are affected by various factors and interests.\textsuperscript{312} Therefore, it is necessary to use context-sensitive approaches to explore the factors that affect ‘law in action,’ especially criminal justice systems under the context of globalisation.\textsuperscript{313} Banakar posited that ‘the method of contextualization situates legal action, behaviour, institution, tradition, text, and discourse in specific time and socio-legal space, thus revealing law’s embeddedness in societal relations, structures, developments, and processes.’\textsuperscript{314}

The use of socio-legal methods in comparative law research is highly necessary because ‘it goes beyond doctrinal issues and span very different cultural contexts....’\textsuperscript{315} Applying both doctrinal and socio-legal methodologies make this research more interesting and meaningful because together they help to systematically evaluate and interpret the legal rules and practices contained in the anti-terrorism laws of the two jurisdictions.\textsuperscript{316}

3.5 Conclusion

This chapter has outlined that this thesis mainly uses a combination of doctrinal, comparative and socio-legal methodologies in pursuit of its research purposes. The doctrinal method is applied to comprehensively examine existing anti-cyberterrorism legislation and the legal systems underpinning it in both jurisdictions, as well as relevant scholarly documents, NGO reports, and court decisions. In addition, the comparative method is employed to critically and comprehensively evaluate the legal responses to cyberterrorism in China and E&W to identify divergences and

\textsuperscript{312} D Nelken, \textit{Comparing Legal Cultures} (Dartmouth 1997); D Nelken and J Feest (eds), \textit{Adapting Legal Cultures} (Hart Publishing 2001); D Nelken, ‘Using Legal Cultures: Purposes and Problems’ in D Nelken (ed), \textit{Using Legal Culture} (Wildy, Simmonds and Hill 2012) 1-51.


\textsuperscript{316} The synthesis of the doctrinal (Black-letter) approach and socio-legal is not only possible within a comparative legal research, but also gives birth to the ‘contemporary interdisciplinary approach which is able to comprehensively coincide with contemporary trends in legal methodology’. V Levičev, ‘The Synthesis of Comparative and Socio-Legal Research as the Essential Prerequisite to Reveal the Interaction of National Legal Systems’ (The Interaction of National Legal Systems: Convergence or Divergence? International Conference of PhD Student and young Researchers, Vilnius, Apr 2013)163-170.
convergences therein. Ultimately, socio-legal method is used to closely consider the similarities and differences in the above-analysed areas with respect to their legal systems and draw the following conclusion for this article: the substantive relations of connection between a legal system and legal responses to cyberterrorism is contingent rather than necessary.
Chapter 4 The Legal System in China

4.1 Introduction

This thesis attempts to undertake a comparatives study of the legal responses to cyberterrorism of China and E&W, and then figure out whether the relationship between the legal systems and the legal responses is necessary or contingent with respect to counter-cyberterrorism. Accordingly, this chapter aims to provide an overview of the core elements of “rule by law” and basic criminal law principles in China because this provides a foundation upon which to establish whether the distinctive legal system of China contributes to explaining its legal responses to global uncertainties like cyberterrorism.

The contents of the chapter are mainly divided into two parts. Firstly, this chapter starts by outlining the differences between the definitions of “rule of law,” “rule by law” and “rule of man.” Although the CCP proclaims that China is a “socialist rule of law country” and introduced the notion of “rule of law” into the Constitution in 2004, its version of this is quite different from its Western liberal democratic counterparts. Crucially, the distinctive characteristics of the legal system in China are referenced in the Constitution’s text which states “rule of law with Chinese characteristics.” In reality, this is actually “rule by law,” which means the CCP has supreme power, concentration of powers, there is a lack of judicial independence, different understanding of human rights protection, and there is a lack of checks and balances on human rights protection. The State’s power is equivalent to that of the CCP, and the law is used as a tool to achieve the Party’s goals and to restrict civic behaviour rather than state power. These distinctive characteristics continue to determine the country’s legal response to cyberterrorism.

Secondly, since criminal law plays a key role in combating cyberterrorism in China, this chapter also tries to set out the basic legal principles in criminal law in China. Applying existing anti-terrorism legislation to combat cyberterrorism also reflects the characteristics of “rule by law” whereby China prioritises the protection of national security, social stability and collective rights. The lack of counterbalance here may
result in violations of the principles of proportionality, certainty of law, minimal criminalisation and legality. Moreover, in this chapter, I will discuss the legal response to cyberterrorism in China in relation to these constitutive principles.

4.2 Rule by Law, Rule of Law and Rule of Man

4.2.1 Defining the “Rule of Law” from Western and Chinese Perspectives

The term “rule of law” was coined by Professor Albert Venn Dicey, who used it in his book *An Introduction to the Study of the Law of the Constitution* in 1885. It has been written that he ‘associated the rule of law with rights-based liberalism and judicial review of governmental action.’317 Dicey’s interpretation of the rule of law consists of three central principles:

Firstly, no man is punishable or can lawfully be made to suffer in body or goods except for a distinct breach of law established in the ordinary legal manner before the ordinary courts of the land... Second, equality before the law... thirdly, the Constitutions are not the source but the consequences of the court’s definition and enforcement of individual rights... 318

China and the West have different understandings of the “rule of law.” The rule of law is a product of Western liberal democratic philosophy, outlined by Edward Craig as follows:

Most simply expresses the idea that everyone is subject to the law, and should therefore obey it. Governments in particular are to obey law—to govern under, or in accordance with law. The rule of law thus requires constitutional government, and constitutes a shield against tyranny or arbitrary rule: political rulers and their agents (police and so on) must exercise power under legal constraints, respecting accepted constitutional limits.319

---

Since “rule by law” (法制) and “rule of law” (法治) are both translated as fazhi in Chinese, there is much confusion among the public. Rule by law has two meanings in Chinese discourse: “legal system” and “ruling the country according by laws.” Contrary to rule of law or rule by law, rule of man (renzhi, 人治) means that the rule of the State is based on the ruler rather than the law, and the law is used to rule the ordinary people rather than the ruling class. Most of Chinese scholars believe that the rule of man has been abandoned by China, but still disagree with the supremacy of law or worship of law, because the law cannot conflict with the leadership of the CCP.320 Although these scholars have already known the difference between rule by law and rule of law321, they hold the view that the rule of law cannot be achieved overnight, and instead needs to follow a cautious path from legalisation to rule by law, and then to the rule of law.322 These scholars have claimed that rule by law (i.e. ruling the country according to a set of laws by institutional authority rather than by an individual leader), was moving China inevitably towards the rule of law.323 Under the legal system of rule by law, the law is a tool in the hands of the rulers used to pursue their goals, and they themselves are not bound by the legal system. For instance, Guo Daohui stated that two points are significant when distinguishing rule of law from rule by law: whether law is supreme or whether it is used as an instrument.324 Some scholars consider that establishing a democratic rule of law requires the following three conditions: a coherent legal system; an independent judiciary; and legal awareness of the general public. Without political democracy and judicial independence, the rule of law would be

321 In June 1990, the Shanghai Academy of Social Science co-held a symposium with the Princeton University, USA, on the following topic: “Theory and practice of the rule of law in the USA”. The participants concluded from this discussion that rule by law was not equal to the rule of law even if it included the 16 characters of Deng Xiaoping, but a socialist rule by law was equal to a socialist rule of law. See Zhou Yongkuan, ‘Review of the Symposium on Administering the State According to Law and Building up a Socialist Country based on the Rule of Law(依法治国,建设社会主义法治国家理论研讨会书评)’ (1997) 2 Rule of Law and Social Development 12-14.
324 Yu Xuede, ‘Rule of law or rule by law, governing the people or governing the power? a summary of debates on the issue of governing the state according to law（法制还是法治，治民还是治权:关于依法治国问题讨论观点综述）’ (1997) 12 The Front Line 26.
nothing but empty talk. Some scholars claim that the “supremacy of the CCP” is the greatest obstacle to achieving the rule of law in China. Indeed, some Chinese scholars in Western countries have critically asserted that the CCP regards law as a tool to realise its policies and to maintain social stability and unity. Peerenboom concluded that in contemporary China, the Party continues to exert influence or interference in the legislature and courts, depriving citizens of many civil and political rights, and severely suppressing ideological dissidents, any autonomous organisations, and especially the voicing of political opposition on the Internet.

Compared to the Western liberal democratic version of the rule of law, the socialist rule of law is quite different, and is more akin to rule by law. Who should be ruled is the fundamental difference between rule by law and the rule of law. China’s 1982 Constitution was revised in 1999 when a new paragraph related to rule of law was adopted, the current Article 5, which states: ‘The People’s Republic of China governs the country according to law and makes it a socialist rule of law country.’

Chinese and official propaganda department are very optimistic that the Chinese legal system adopts “rule of law” because the Chinese term “fazhi” is translated into Western term “rule of law.” Many Westerners are sceptical about the official Chinese translation of “rule of law.” Harro von Senger, a senior sinologist, believed that the term “rule by

---

329 China’s Constitution, Article 5.
law” reflected the legal reality in China better than “rule of law.” A key requirement of the rule of law is the separation of state power from party power, but China's state power is exercised by the only ruling party (the CCP) on behalf of the people. In this sense, the law is used to restrict civic behaviour rather than to consolidate state power. The ”rule by law” reality shapes the way in which Chinese anti-terror legislation is formed and implemented. The current purpose of the CCP is mainly to focus on national security and maintaining social stability. Indeed, the current focus of the CCP is mainly on national security and maintaining social stability. Therefore, using existing laws to combat cyberterrorism also reflects China’s commitment to this end.

However, after decades of legal reform and institutional development, the Chinese government has not only tried to establish a comprehensive legal system and legalise the administration, but it has also attempted to impose a certain degree of meaningful restrictions on government officials and members of the CCP. In the process of legal reform, the CCP’s governance methods have undergone significant changes. The Party mainly governs through policies in the form of documents or internal rules circulated within administrative agencies. These documents or rules are so abstract and general that they can be applied and changed flexibly. Currently, the CCP and the Chinese government are trying to establish a general separation, which would act as an effective legal framework on the basis of clear, stable and forward-looking laws, replacing political policies and rules in the operations of the State. China is increasingly becoming subject to a series of laws rather than the Party’s policies. The ongoing legal reforms are placing more legal restrictions on government power. At the same time, the Chinese government has long recognised that public power must be restricted to deal with potential problems such as corruption, environmental degradation and illegal land acquisition, even if this can incite social unrest and challenges to social and political stability.

---

334 Ibid.
4.2.2 The Chinese Socialist “Rule of Law” or “Rule by Law”

Through an examination of the legal systems in China and E&W, it could be observed that the rule of law is understood and interpreted differently to the point that one should categorise them into “Western rule of law” (E&W) and “rule by law” (China). The Western version of the rule of law contrasts sharply with the understanding of the rule of law with Chinese characteristics: instead of a separation of power which would be intended to limit the power of the state organs, China adheres to the principle of democratic centralism with power concentrated in the hands of the CCP. Consequently, there is a lack of supremacy of law and substantive judicial independence in China where all state organs (executive, judiciary, legislature) should follow the law under the control and guidance of the CCP (shown in figure 4.1).

Figure 4.1: China’s Political Structure: The Communist Party sits atop China’s political power structure, controls all legislature, executive and judicial institutions, and commands the military.

In 1997, the term “rule of law” first appeared in official Chinese texts, after being proposed at the Party’s 15th Congress as "Yi fa zhi guo, jianli shehuizhuyi fazhi guo" [governing the country according to law and establishing a socialist rule-of-law]

---

country]. On 8 March 2011, Wu Bangguo, Chairman of the Standing Committee of the National People’s Congress (SCNPC), announced ‘A socialist system of laws with Chinese characteristics has been established on schedule in China.’ It has been suggested that the term “socialist” embodies an “anti-individual” element and a disposition against “the fundamental concept of personality.” Since the term “socialist” is a political or ideological concept, it also implies that the Chinese rule of law serves “collective interest” rather than individual human rights. This further shows that China and E&W use the rule of law to achieve different goals. While the rule of law is meant to ensure the liberty and equality of people in E&W, the rule of law with Chinese characteristics (or rule by law) is applied to ensure economic and social development as well as stability and security in society.

Although the 1982 Constitution (China’s current constitution) adopted basic principles of the rule of law, China is still far from being a rule of law country according to the observations and examinations of some scholars in both China and the West. According to Keith, China’s *fazhi* (“rule of law”) is actually rule by law rather than the genuine rule of law, although both have the same pronunciation in Chinese. Tony Saich, meanwhile, claimed that a socialist rule of law had always run through the entire process of legal reform in China, with the CCP essentially determining what is and what is not a crime. Some scholars consider that the rule of law would be impossible

---

338 Jiang Zemin, ‘Upholding the great banner of Deng Xiaoping theory to fully push the establishment of socialism with Chinese characteristics into the twenty-first century’ (1997) 18 Seeking Truth Magazine 3.
339 China’s legislative goal of forming a socialist system of laws with Chinese characteristics by 2010 was set forth at the fifteenth National Congress of the CPC in 1997. On behalf of the SCNPC, Wu delivered a report and claimed: ‘We now have a complete set of types of laws covering all areas of social relations, with basic and major laws of each type already in place, together with comprehensive corresponding administrative regulations and local statutes’, and ‘Overall, the system of laws is scientific, harmonious and consistent.’ Xinhua, ‘Socialist system of laws established in China’ (Xinhua, 10 March 2011) <www.china.org.cn/china/NPC_CPPCC_2011/2011-03/10/content_22099470.htm> accessed 22 March 2019.
343 Such as the supremacy of the law, the equality of all before the law, the need for officials to act accord to the Constitution and the law, and the rights of citizens to enjoy a wide range of freedom. See Art.5 and Art.33 of the PRC Constitution.
to realise in China due to the fundamental incompatibility between a single-party authoritarian government and the rule of law. In addition, Stanley pointed out that the CCP puts social stability and economic development at the forefront, thus creating a policy of “strike-hard campaigns” and ideological suppression by imposing severe penalties on political and religious heretics and criminals. Even though the CCP uses the term “rule of law” this does not mean that it gives primacy to law above political considerations and the Party’s policy.

The Western liberal rule of law requires ‘the sanctity of individuals in the enjoyment of liberty and property’, and a democratic legal system. These criteria are often used unconsciously to evaluate Chinese law, making it is easy to claim that China’s legal system is only established on the basis of rule of man or, at best, rule by law. However, Since the Deng Xiaoping era (1978-1989), China has felt the need to distinguish its legal system from a ‘rule by man’ structure. Deng Xiaoping realised that China’s long-term stability required the restriction of state power, the separation of government and party power, and the reliance on law rather than a man (leader) to solve problems. Deng Xiaoping stressed that: ‘there must be laws for people to

---


348 During the reform period(1980-1990), three nationwide strike-hard campaigns were indicated in 1983, 1996, 2001, respectively, with numerous small-scale campaigns launched at the local level. Xinhu, “China launched the “Strike Hard Campaign against Violent Terrorism” (严厉打击暴力恐怖活动专项行动) in the far west province of Xinjiang’(Xinhua, 25 May 2014) <http://www.gov.cn/xinwen/2014-05/25/content_2686705.htm> accessed 20 Oct 2020. It included measures targeting cell phones, computers, and religious materials belonging to Uyghurs. The government simultaneously announced a "people's war on terror" and local government introduced new restrictions that included the banning of long beards and the wearing of veils in public places. Official figures show that Xinjiang prosecutors approved 27,164 criminal arrests in 2014, the first year following the announcement of the new strike-hard campaign. This represented a rise of around 95 percent from the previous year. See Yue Ran and Hong Sha(ed), ‘Xinjiang: The number of arrests nearly doubled in 2014 (新疆2014批捕人数增加近一倍 )’(Uyghur Human Rights Project, 24 Jan 2015)< https://chinese.uhrp.org/article/1310080522> accessed 23 Sep 2020.

349 S Lubman, China’s Legal Reforms (Oxford University Press 1999) introduction, 2.

350 T Saich, Governance and Politics of China (Palgrave 2001) 125,126.

351 RC Keith, China’s Struggle for the Rule of Law (Palgrave Macmillan 1994) 7.


follow, these laws must be observed, their enforcement must be strict and lawbreakers must be dealt with. 有法可依，有法必依，执法必严，违法必究’. 355 With this in mind, he believed that the policies and ideology of the CCP should be passed through legislation to justify them, and to regularise state management. Presumably, this was because the Chinese leadership felt there was some need to legitimise its rule, in this instance through making references to what constitutes a socialist legal system rather than an arbitrary dictatorship of a particular individual ruler. This is analytically significant because the rejection of arbitrary executive rule ‘by man’ places some constraints on the legal responses to perceived threats such as cyberterrorism.

Different understandings of the rule of law affect the relationship between the people and state organs in many ways, as well as the distribution of power and the protection of human rights to different degrees. In light of this, a question emerges as to whether the different understanding of the rule of law affect the approaches in the context of countering cyberterrorism. This question will be analysed in chapter eight.

The comparison of legal regimes indicates that despite their different understandings of the rule of law, there does appear to be some convergence with respect to their legal responses to cyberterrorism. Both China and E&W have a similar “rule by law” tendency in the context of combating cyberterrorism. The imprecision of “rule by law” underpins a more authoritarian approach, which is justified in terms of the need for more preventive or pre-emptive interventions against online preparatory terrorist activities in both jurisdictions. This convergence can also be illustrated through reference to the Prevent and Persue strands of the CONTEST program adopted by E&W, and China’s preventive strategy.

Furthermore, the notion of “rule of law” entails a series of key constitutional elements to guarantee the fundamental human rights of the people. As shown in the following chart (figure 4.2), the comparison of these key factors reflects the vastly distinctive impacts of anti-terrorism laws in the corresponding jurisdictions.

<table>
<thead>
<tr>
<th>E&amp;W</th>
<th>China</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rule of law</strong></td>
<td><strong>Rule by law (法治 fazhi)</strong></td>
</tr>
</tbody>
</table>
| Core elements |  • Supremacy of law  
  • Separation of powers  
  • Independent judiciary  
  • Protection of fundamental individual rights |  • Supremacy of the CCP  
  • Lack of separation of powers  
  • Lack of independent judiciary  
  • Lack of individual rights protection |
| Implications of anti-terrorism laws |  • Independent review system  
  • Judicial review of anti-terrorism legislation  
  • Legislative scrutiny |  • Lack of counterbalance between security and human rights protection  
  • Violation of principles of certainty, proportionality, minimal criminalisation, etc.  
  • Lack of due process and effective judicial review, arbitrariness |

Figure 4.2: key factors of ‘rule of law’ vs. ‘rule by law’ and implications of anti-terrorism laws in E&W and China

For scholars of counter-terrorism legislation and policy, the possibility of tension arising between rule by law and rule of law is well-known. The rule of law contrasts with arbitrary power while, rule by law, on the other hand, involves cloaking arbitrary power in legal formalities. Overzealous anti-terrorism legislation also poses some problems for the rule of law. Essentially, applying preventive anti-terrorism laws to combat cyberterrorism runs the risk of creating rule by law rather than the rule of law.

### 4.3 Distinctive Characteristics of the Legal System in China

In order to explore the relationship between the legal regime and specific legal responses to cyberterrorism in China and E&W, it is first necessary to compare the core elements of the two legal systems. In particular, the following core elements are of great relevance to anti-terrorism laws: separation of powers; rule of law; judicial

---

independence; and human rights protection. These are analysed in detail below.

4.3.1 Concentration of Powers

The separation of powers is a cornerstone of E&W’s legal system, while in China there is a division of duties instead of a separation of powers. China is an authoritarian state in which a strong central government and administrative divisions exercise power on the State’s behalf. Unlike E&W, in China’s division of state organs (such as the executive branch, the judicial branch, the legislative branch, and the supervisory branch) the emphasis is placed on the differentiation of responsibilities, rather than the separation of powers. According to the CTL, the departments related to counter-terrorism prefer cooperation rather than supervision and restriction of power. For instance, after several serious terror attacks in 2014, the National Counter-terrorism Work Leading Organ (hereafter, the Organ) drafted the Counter-Terrorism Law in cooperation with other departments, including the National People's Congress Law Committee, the Ministry of State Security, the Ministry of Industry and Information Technology, the People's Bank of China, the Legal Affairs Office of the State Council, and the Armed Police Headquarters. Consequently, the Organ became the institution that bears the responsibility for identifying terrorist activities, organisations and individuals and managing inter-agency counter-terrorism coordination across the country.

The leaders of the CCP have always been hostile to the separation of powers. Even

---


359 Art. 8 of CTL states that all kinds of anti-terrorism related departments should implement a work responsibility system based on division of labor.

360 National Counter-terrorism Work Leading Organ: 国家反恐怖工作领导机构


362 Jiang Zemin, ‘Upholding the great banner of Deng Xiaoping theory to fully push the establishment of socialism with Chinese characteristics into the twenty-first century(高举邓小平理论的伟大旗帜，把建设有中国特色的社会主义全面推向21世纪)’ (1997) 18 Seeking Truth Magazine 3.
the great reformer Deng Xiaoping who adopted many things from the economically successful Western world, believed that Western democracy and the separation of powers was unsuitable for China's national conditions. China’s Constitution has granted eternal and unchangeable leadership to the CCP, which thereby still stands above the law. Since the Deng Xiaoping and post-Deng era (1978-2013), China’s legal system has undergone huge improvements such as the separation of the CCP and government, which represented the rule by law stage. However, since Xi Jinping took over in 2013, the CCP has re-established its concentration of power.

However, since 1989, Deng Xiaoping later changed his mind and believed that the idea of separation between the party and the government was a manifestation of “bourgeois liberalization.” A basic strategy adopted by the CCP is to incorporate party policies into national laws through legal procedures, and then the Party takes the lead in complying with these laws in the Constitution. By doing so, the Party’s leadership is strengthened and the Chinese government’s efficiency is improved because these laws are based on the Party’s lines, policies and goals. The development of China’s legal system shows that the authorities feel the need to distinguish the legal system from a rule by man approach, presumably because the leadership feels there is some need to legitimise its rule, in this instance through making references to what

363 Deng Xiaoping held: “In developing our democracy, we cannot simply copy bourgeois democracy, or introduce the system of separation of powers. [...] We cannot do without dictatorship.” Quoted by BL Milkwick, ‘Feeling for Rocks while Crossing the River: The Gradual Evolution of Chinese Law’ (2005) 14 TLP 304.
364 Para. 7 of preamble of the Chinese Constitution.
constitutes a socialist legal system rather than an arbitrary dictatorship of a particular individual ruler. In this context, China tries to legitimise its anti-terrorism approaches to its citizens. Accordingly, China’s approaches to terrorism are a codification of collective will, that is the collective interests of national security and social stability.

In E&W, the aim of the separation of powers is to prevent the abuse of state authority through applying checks and balances. However, China has not introduced the substantial separation of powers exercised in the West. Instead of a separation of powers, China has applied democratic centralism (minzhu jizhongzhi) and division of duties. Unlike E&W, the division of state organs (such as executive branch, judicial branch, legislative branch, supervisory branch) emphasizes the differentiation of responsibilities, rather than the separation of powers. The legislative organ, the National People’s Congress (NPC), is nominally the highest state power, which generates and supervises the other two state powers (the executive and the judiciary). However, in fact, the power of these three state organs is ultimately concentrated in the hands of the CCP as China continues to resist adopting the Western ideas of separation of powers and judicial independence. For instance, according to the CTL, the departments related to counter-terrorism prefer cooperation rather than supervision and restriction of power.

Therefore, due to its current political status and legal structure, China does not have substantive judicial independence. Accordingly, with regard to the implications of

---

372 According to the Chinese Constitution, all state power belongs to the people and must be exercised through the NPC and local people’s congress at various levels(Art.2). "Democratic centralism(minzhu jizhong zhi)", rather than separation of powers, is a guiding principle of the Constitution. Under the principle of "democratic centralism", the NPC is the highest organ of state power(Art.57). The central government (State Council) and the two supreme judicial authorities (the SPC and the SPP) are therefore generated and supervised by the NPC.
374 Art.8 of CTL states that all kinds of anti-terrorism related departments should implement a work responsibility system based on division of labor.
counter-terrorism legal approaches, China lacks effective judicial review and checks and balances to prevent abuses of state power and arbitrariness, thereby leading to unrestricted violations of individual rights. Meanwhile, E&W can prevent abuses of state power through effective judicial oversight legislation and executive power in its corresponding counter-terrorism measures (for example, judicial review of control orders by the court, an independent review system of anti-terrorism law, and the implementation of the control order being reported to the Parliament).

4.3.2 Lack of Judicial Independence

Both E&W and China embrace the principle of judicial independence, but their interpretations of this principle are very different. In E&W, judicial independence is based on the principles of rule of law and separation of powers. The judicial power is vested in judges who are independent and the judges are subject only to the law. Judicial independence protects the judiciary from infringements by the legislative and executive branches, thus constituting a bulwark against any abuse of power. Meanwhile, in China, due to the centralisation of power, Chinese judges do not enjoy the substantial independence.

Art.126 of the Chinese Constitution provides for judicial independence as a constitutional principle.\(^{375}\) On paper, Chinese judges seem to have the same independence as the West. However, due to many political and practical factors, Chinese judges are not afforded such independence in practice. Notably, Chinese courts and judges continue to be subject to various outside influences, particularly to the control of the CCP. Jiang Huiling, a former judge at the Chinese Supreme People’s Court (SPC), described four channels of interference into the work of Chinese courts.\(^{376}\) First, she claimed that the courts are often confronted with interference from people’s congresses or government entities.\(^{377}\) Second, courts are financially

---

\(^{375}\) Art. 126 of Chinese Constitution: “The people’s courts shall, in accordance with the law, exercise judicial power independently and are not subject to interference by administrative organs, public organizations or individuals.”


\(^{377}\) Wang Chenguang, ‘From the Rule of Man to the Rule of Law’ in Cai Dingjian and Wang Chenguang (eds), *China’s Journey Towards the Rule of Law—Legal Reform 1978–2008* (Brill 2010) 31. Article 128 of the Chinese Constitution clearly stipulates that courts are responsible to the People’s Congresses at the
dependent on the corresponding level of local government for salaries, housing, benefits, and so forth. Third, the people’s procuratorates exercise legal supervision over the courts. Finally, in many cases, decisions of judges or panel must be submitted to chief judges or to the president of the court for approval. Sometimes, they are decided by the court’s adjudication committee which comprises a group of people who did not take part in the trial. All of these factors clearly give rise to political interference. When adjudicating cases, an individual judge is subject to the control of his or her leaders in the court, and the court, in return, is subject to the leadership of the local CCP Committee through its Political and Legal Committees (PLCs).

4.3.3 Different Understanding of Human Rights Protection

Under the Western understanding of the rule of law, the protection of human rights is fundamental. Human rights law generally endorses the principle of proportionality: any interference with human rights in the name of, for instance, national security or social stability, must be proportionate. However, China does not have domestic human rights laws that follow the structure of international human rights law, and so it is necessary to investigate whether China nonetheless follows the principle of proportionality when using its existing legislation to counter cyberterrorism.

Domestically, human rights have been entrenched in the Chinese Constitution since 1982. In 2004, the Constitution was amended to provide expressly that ‘the state respects and [safeguards] human rights.’ Internationally, China voted together with

---

379 Chinese Constitution, Article 129.
380 These committees, composed of serious of senior judges, division chiefs, and court leaders are responsible for summing up adjudication experiences, discussing major or difficult cases and other adjudication-related matters, in conformance with the principle of “democratic centralism”. See in detail Jiang Huiling, ‘Judicial reform’ in Cai Dingjian and Wang Chenguang (eds), China’s Journey Towards the Rule of Law—Legal Reform 1978–2008 (Brill 2010) 205.
382 See China’s Constitution, Arts. 33-56.
383 Ibid.
the US in favour of the 2012 resolution of the United Nations Human Rights Council to protect the free speech of individuals on the Internet, which directly addressed the right to freedom of expression and opinion on the Internet.384 Although China has made some progress in its human rights protections, its approaches to human rights have reflected values and mentalities that are rather different from those of the Western world.385 Pertinently, the Chinese government has claimed that ‘no country in its effort to realize and protect human rights can take a route that is divorced from its history and its economic, political and cultural realities.’386

In China, the human rights values explicitly granted by the Constitution are restricted in reality.387 Therefore, the understanding of human rights in China is based somewhat on obligation, which means individual rights are considered subordinate to the needs and demands of national interests and social stability. For example, the Chinese government on 18 March 2019 issued the Counterterrorism and Human Rights Protection White Paper, saying that the country attached top priority to a preventive counterterrorism approach.388 China’s basic stand on the development of human rights is: ‘prioritising people’s rights to subsistence and development, making

387 Art.51 of Chinese Constitution: “Citizens of the People’s Republic of China, in exercising their freedoms and rights, may not infringe upon the interests of the state, of society or of the collective, or upon the lawful freedoms and rights of other citizens.”
388 “Based on the experience of absorbing the anti-terrorism experience of the international community, China actively responds to the UN General Assembly resolution on the UN Global Counter-Terrorism Strategy (60/288) and is committed to ‘eliminating the conditions for the spread of terrorism and preventing and combating terrorism.’ Based on the reality of the region, Xinjiang has carried out in-depth anti-terrorism and de-extremization struggles, adhered to the principle of ‘fighting with one hand and preventing with one hand’, cracking down on violent terrorist crimes in accordance with the law, and attaching importance to the prevention of radicalization of terrorism. Through efforts to improve people’s livelihood, strengthen legal publicity and education, and establish vocational skills education and training centers (hereinafter referred to as “teaching and training centers”) to assist education and other means to maximize the protection of citizens’ basic human rights from terrorism and extremism.” The State Council Information Office published a white paper on "Countermeasures against Terrorism, De-extremization and Human Rights Protection in Xinjiang", (Xinhua,18 Mar 2019)<http://www.gov.cn/zhengce/2019-03/18/content_5374643.htm> accessed 7 Aug 2019.
development the principal task, then promoting citizens’ political, economic, social and cultural rights'.

China's human rights philosophy is reflected in its approach to Internet governance, which has been largely state-centric and accentuates the individual's responsibilities over the individual's rights. China's laws and policies to combat cyberterrorism in some way reflect China’s perspective and philosophy on human rights. For example, according to its cybersecurity law, on the one hand, it pledges to unconditionally protect the privacy and individual data; on the other hand, it also gives the Chinese government or third parties great power to infringe upon the privacy of citizens. Clearly, the fundamentals and principles of China’s human rights are significantly different from those of E&W. In E&W, from their very introduction, human rights have been designed to protect individuals from state power. However, China has viewed human rights as something that is derived from the State, which reigns supreme over the individual. Hence, China holds the view that national or collective interests take precedence over individual rights, meaning that when national or collective interests conflict with individual rights, the latter can be sacrificed. In the context of combating cyberterrorism, China prefers a control model which safeguards national security and social stability, and where public life and property security are regarded as the foremost goals above the protection of individual rights. Compared to China, Western countries place a greater emphasis on the due process model, in which the fundamental goal of the legal system is to protect individual rights, including defendants’ rights. China has developed an increasingly sophisticated approach to free speech, taking into account the free flow of information, an individual's reputation, privacy and the nature

391 China’s Cyber Security Law.
393 "China is a high context society in which most people share a common set of norms, values, and beliefs." DCK Chow and AM Han, Doing Business in China: Problems, Cases, And Materials (West Academic Publishing 2012) 692-93
of social media.395 However, the Chinese government still strictly controls speech online, especially anything relating to political dissent, terrorism, extremism and separatism as the exercising of human rights is not allowed to threaten the regime or social stability. Despite the Chinese government’s ongoing efforts to strengthen the human rights protection it provides, the State’s own actions are largely unrestricted by fundamental human rights.

Moreover, there is a close tie between the State and academia in China. For example, with regard to legal responses to terrorism issues, many scholars accept the official discourse without criticism, leaving issues such as human rights violations unaddressed.396 Although some Chinese scholars have tried to criticise the State on some issues related to counter-terrorism, such as the practice or principles of “combining leniency with severe punishment,”397 “pocket crime,”398 and “the hard approach,”399 these criticisms have not been enough to influence the CCP to change its anti-terrorism laws. Meanwhile, the current legal approaches to cyberterrorism in E&W have been the subject of considerable criticism, much of which has focused on the tension between the imperative of prevention and early intervention and the impact on human rights and the rule of law of excessively broad and vague criminal offences.400

Obviously, there is no uniform standard to regulate individual rights universally in terms of the extent to which state organs and citizens should be restricted. Therefore, this arduous task has been left to the courts. In particular, in the context of counter-terrorism, individual rights in both China and E&W have been derogated. There has been a creeping erosion of liberty courtesy of the passing of numerous expansive anti-terrorism acts — each of them seem harmless, but together they add up to a ‘formidable armory of state powers.’401 The biggest difference between China and

396 The details could be found in Literature Review Chapter.
400 The details could be found in Literature Review Chapter.
E&W in this regard is still the role of the courts. China does not have a constitutional court, which means that judges cannot directly invoke the Constitution when ruling, so they cannot examine whether the legislative and administrative acts are in compliance with the Constitution in terms of human rights protection.

In order to effectively combat the threat of terrorism, the legal responses of the two countries have become proactive. Due to the devastating consequences of contemporary terrorism, many states are no longer satisfied with prosecuting terrorist attackers ex post. On the contrary, they consider it crucial to prevent the perpetrators from carrying out terrorist activities in the first place and thus take action proactively. A side-effect of this approach is that human rights are increasingly restricted. Although a heavy emphasis on security and public interest is imperative for effective counter-terrorism, anti-terrorism campaigns cannot completely ignore human rights protection. The lack of counterbalance here further exposes the reality of “rule by law” in China. I argue that it is not sufficient to merely mention in Chinese law that counter-terrorism work should respect human rights. Indeed, the neglect of the principle of proportionality, the lack of precision in the language of the law and the lack of due process and effective judicial review are fundamental issues which preclude China from genuinely achieving the rule of law.

4.3.4 Lack of Checks and Balances on Human Rights Protection

In Western democracies (such as E&W), human rights protection is ensured through checks and balances. 402 This checks-and-balances mechanism is important to balance national security with human rights. Comparatively, while government surveillance for law enforcement or national security purposes is common in E&W, the implementation of such surveillance is usually subject to various levels of scrutiny in order to balance different interests, especially those concerning criminal investigations, national security, privacy and civic liberties. For instance, according to the Prevention of Terrorism Act 2005 in E&W, the Intelligence Services need to obtain a warrant to

conducted activities domestically as well as overseas.\(^{403}\) By contrast, since China has neither effective checks and balances nor judicial independence,\(^{404}\) so if the administrative agencies violate personal privacy or other rights in the context of combating cyberterrorism or safeguarding national security and social stability, the court cannot constrain the administrative agencies for abusing their power. It is difficult to seek judicial remedies in the courts. For example, the Cybersecurity Law (CSL) provides various provisions that enable the Chinese government’s surveillance and control over information without substantial constraint.\(^{405}\)

In addition, the courts have no power to review government violations of human rights in accordance with the Chinese Constitution, nor does any independent institution review the state organs’ compliance with the Constitution,\(^{406}\) and citizen’s human rights remedy channels have not been effectively safeguarded by courts in reality.\(^{407}\) According to the newly-published white paper and report from the SPC, the CCP emphasises that ‘China respects and protects human rights in accordance with the principles of its Constitution… it is in keeping with the purposes and principles of the UN to combat terrorism and safeguard basic human rights.’\(^{408}\)

Therefore, although both China's Constitution and anti-terrorism laws stipulate that human rights should be respected and protected, and that counter-terrorism legislation has far-reaching human rights impacts\(^{409}\), China lacks an effective judicial review

---

403 See the Intelligence Services Act was amended by the Prevention of Terrorism Act 2005, which provides the Intelligence Services authority to obtain a warrant to conduct activities in the UK as well as overseas. The Security Service also can obtain a warrant to interfere with property or wireless telegraphy if the action proposed is to be "undertaken otherwise than in support of the prevention of detection of serious crime Intelligence Services Act 1994, s 5(4), (5).


406 Therefore, Zhang Qianfan suggests the establishment of an independent committee under the NPC. See K Blasek, 'Rule of Law in China: A Comparative Approach' (Springer 2015) 51.

407 See Art. 90 para. 2 of the Chinese Legislation Law: “any citizen can only suggest the SCPC to deal with a certain issue or critic on legislation. But the actual dealing or decision cannot be claimed by citizens.”


409 Such as the designation of individuals or groups as terrorist.
mechanism like that of E&W in its legislative provisions and practices. In my opinion, the lack of any independent counterbalance not only indicates that Chinese anti-terrorism legislators have chosen to prioritise the public interest over individual human rights, but it also seems to suggest that the lawmakers simply do not see any significant need to strike some kind of balance between the two.

A good example illustrating the different views of China and its Western counterparts on human rights protection is the case of Apple vs. Federal Bureau of Investigation (FBI).\textsuperscript{410} In this case, Apple declined to assist law enforcement personnel to decrypt a suspect's iPhone initially, after which the Department of Justice obtained a warrant from court which was challenged by Apple.\textsuperscript{411} However, in China’s case, the CSL and CTL do not restrict the Chinese government's power to gain assistance in decryption. Moreover, the administrative organs in China request relevant ISPs to provide individual information, decryption or other technical support without a warrant. Ultimately, both anti-terrorism legislation and the Judiciary have neglected the safeguarding of human rights in China.

The prevention strategy has been used as a tool of abuse and is justified in the name of counter-terrorism. Although the legislation and policy of both China and E&W make explicit commitments to protecting fundamental freedoms and core values, there are significant gaps in actualising anti-terrorism measures. The UK has stronger judicial oversight, legislative scrutiny and independent review mechanisms for anti-terrorism approaches than China where the oversight mechanisms are mostly within the executive branches. It is arguable that the enactment of overly broad anti-terrorism laws in E&W carries the risk of rule by law materialising, with the rule of law being undermined.


4.4 Basic Criminal Law Principles in China

Criminal law plays an important role in dealing with the threat of terrorism, and many governments have come to regard it as the main response to such an threat.\(^{412}\) China is no exception, relying mainly on criminal law to fight cyberterrorism. The basic principles of criminal law, as the basis of legal norms, reflect the legislative values commitment and the basic spirit and direction of law enforcement interests.\(^{413}\) Therefore, it is necessary to figure out what the basic principles of Chinese criminal law are and what sorts of offences are considered crimes, as is stipulated in Chinese Criminal Law 1997, Art. 13:

All acts that endanger the sovereignty, territorial integrity, and security of the state; split the state; subvert the political power of the people's democratic dictatorship and overthrow the socialist system; undermine social and economic order; violate property owned by the state or property collectively owned by the laboring masses; violate citizens' privately owned property; infringe upon citizens' personal rights, democratic rights and other rights; and other acts that endanger society, are crimes if according to law they should be criminally punished. However, if the circumstances are clearly minor and the harm is not great, they are not to be deemed crimes.\(^{414}\)

Additionally, the criminal law task\(^{415}\) is to create a criminal punishment that can be used to combat criminal actions and protect national security, the existing political system, social and economic order, property, and citizens' rights. This implies that by applying the existing criminal law to combating cyberterrorism, China also reflects this value orientation whereby terrorism prevention takes precedence over individual rights.

---


\(^{414}\) China’s Criminal Law, Article 13.

\(^{415}\) The tasks of the PRC Criminal Law are to use punishment struggle against all criminal acts to defend national security, the political power of the people's democratic dictatorship, and the socialist system; to protect state-owned property and property collectively owned by the laboring masses; to protect citizens' privately owned property; to protect citizens' right of the person, democratic rights, and other rights; to maintain social and economic order; and to safeguard the smooth progress of the cause of socialist construction. See Article 2 of Criminal Law.
The direct reflection of “rule by law” in the criminal law contains some of the following basic principles: proportionality; certainty of law; legality: *nullum crimen sine lege* ("no crime without law"); *nullapoena sine lege* ("no punishment without law") and minimal criminalisation.

4.4.1 The Principle of Proportionality

The principle of proportionality, also widely recognised as “suitability” and “necessity,” is another extremely important factor derived from the rule of law. Moreover, this principle also requires fair punishment, which means that criminal punishment and criminal responsibility should fit the crime. In order to achieve proportionate punishment, the severity of the offence and the blameworthiness of the offender should be taken into account. In other words, the severity of offences should be commensurate with the severity of punishments for related crimes.

The principle of proportionality is regarded as an essential element of the “rule of law” stipulated by Art. 5 of the Chinese Constitution. In terms of criminal law in China, the principle of proportionality is stipulated in Art. 5 of Chinese Criminal Law: ‘the severity or leniency of punishment shall be proportionate to the crime committed by the criminal and the consequent criminal liability [prescribed by law].’

This provision is generally considered the principle of commensurability (*zuixing xiang shiyong* 罪刑相适应 or *zuixing jinsheng* 罪刑均衡). The principle of proportionality in China is fundamentally based on the theory put forward by the Italian scholar Cesare Beccaria in his pioneering work *Crimes and Punishments*. According to Wang
Hanbin’s explanation of the NPC, the reason for introducing this principle in criminal law is to ensure that serious crimes are severely punished and misdemeanours are handled more leniently. It also ensures a balance between various provisions of law when punishing crimes. Therefore, this principle includes the following aspects: firstly, the principle of proportionality is the basis of the "general provisions" to deal with issues such as criminal preparation, attempted crimes, incomplete crimes, joint crimes, recidivism and voluntary surrender; secondly, the specific provisions of the criminal law is to have a balanced approach in defining punishments for criminal offences according to the seriousness of the crime; and, thirdly, the nature of crime and its social harm are the main factors in judicial decisions on punishment. Therefore, crimes that endanger national security and social stability (such as cyberterrorism) are more severely penalised than ordinary crimes.

Despite many improvements in the current Criminal Law 1997 in terms of introducing more leniency, commentators believe that the law is still weak in terms of elaborate and detailed provisions on aggravating and mitigating circumstances and thus a proper application of the principle of proportionality remains a crucial hurdle in the actual operation of the law.

In the next chapter, I examine the extent to which the existing anti-terrorism legislation violates the principle of proportionality. Upon closer analysis, we can observe that the existing anti-terrorism legislation is characterised by three major issues that raise concern regarding their impact on the principle of proportionality. Firstly, China’s counterterrorism legal framework still relies on a punitive strategy which pursues punishment over and above what is necessary or appropriate. China has intensified its punishment of terrorism-related perpetrators, to the point that the proposed penalty may not be commensurate with the seriousness of the offence. Secondly, in order to

---

424 The detail could be found in Chapter 5.
pursue security and prevention, the individual’s human rights have been curtailed disproportionately in the name of counter-terrorism. Thirdly, a lack of proximity to the commission of the ultimate harm and the risk of harm may result in a harsh punishment that may violate the principle of proportionality.

4.4.2 The Principle of Certainty of Law

A core requirement of the rule of law is that citizens can predict whether their actions are in accordance with the law. In this sense, the principle of certainty of law could be regarded as a sub-principle of the rule of law, which requires that parliamentary laws and administrative regulations must be sufficiently clear and certain. In terms of criminal law, the principle serves two main functions: first, everyone can predict what conduct is prohibited and punishable; and, second, criminal responsibility is pre-specified by the legislature. The principles of maximum certainty is seen as one of the constituents of the principle of legality, and it has a close relationship with the principle of the non-retroactivity principle. In fact, vague laws may operate retroactively, because no-one is quite sure whether the given conduct is within or outside the rule.

It is a legal ideal that requires criminal offences and penalties to be clear in order to enable citizens who wish to obey the law to understand them and be confident that they will not unwittingly break the law.\textsuperscript{425} However, the Strasbourg Court has also recognised that some vagueness is inevitable in order 'to avoid excessive rigidity and to keep pace with changing circumstances' and that a reasonable settled body of case law may suffice to reduce the degree of vagueness to acceptable proportions.\textsuperscript{426} In addition, the criminal law must be accessible to the public. In this way, the public is thus able to distinguish between lawful or unlawful acts. Moreover, the criminal law has to clearly define criminal offences and their respective punishments. Lord Bingham specified the guiding principles as follows: ‘No one should be punished under a law unless it is sufficiently clear and certain to enable him to know what conduct is forbidden before he does it; and no one should be punished for any act which was not

\textsuperscript{426} Kokkinakis v Greece (1993) 17 EHRHR 397, para 40.
clearly and ascertainably punishable when the act was done.\textsuperscript{1427} 

In China, the Constitution has not explicitly introduced certainty of law as a basic principle. Instead, it is mainly discussed by scholars within the scope of criminal law.\textsuperscript{428} In the context of Chinese Criminal Law, it is widely regarded as the core requirement of the principle of legality in Art.3 of Chinese Criminal Law: ‘For acts that are explicitly defined as criminal acts in law, the offenders shall be convicted and punished in accordance with the law; otherwise, they shall not be convicted or punished.’\textsuperscript{1429} 

According to the 2007 annual report of the Congressional-Executive Commission on China (CECC), many provisions related to “national unity,” “internal security” and “social order” were adopted into Chinese law. These ambiguous provisions give security officials unconstrained legal discretion and can exercise this discretion against those who pose a threat to party leadership. Importantly, a large number of cases in Xinjiang have been based on overly broad criminal provisions involving state security.\textsuperscript{430} 

There are numerous general and vague rules and terms in criminal law which violate the principle of certainty.\textsuperscript{431} Compared with E&W, it seems that common legal provisions in China tend to include ambiguous and abstract terms such as “serious (or flagrant) circumstances” or “other activities (or means).”\textsuperscript{432} These terms are very flexible and vague, thereby providing law enforcement agencies considerable discretion in judicial practice, thus resulting in the arbitrary application of these

\textsuperscript{1427} T Bingham, \textit{The Rule of Law} (Penguin 2011) 55-59. Retrospective punishment is more specifically forbidden under the UN International Covenant on Civil and Political Rights, Art.15. 


\textsuperscript{1429} Art.3 of Criminal Law of PRC. 


\textsuperscript{431} The SPC has undertaken, although without legal foundation, the task of fleshing out these terms through “judicial interpretation” in the forms of “replies” or “opinion”. 

\textsuperscript{432} For example, Art.3b of Counterterrorism Law; Art.120 of Criminal law. The details could be found in Chapter 5.
provisions.

As the abstract nature of all legal norms means that all possible situations are not covered, the principle of certainty does not prohibit the use of general terms such as "public order" and "national security." Therefore, in cases of uncertain legal terms, the judiciary is authorised to flesh them out in legal practice. Although vagueness is not a feature unique to Chinese law, especially criminal law, vague definitions of criminal and non-criminal offenses as well with terms such as “disturbing public order” and “endanger state security” leaving the door open to abuses in the application of the law. 433

In the context of countering cyberterrorism, the current anti-terrorism legislations with respect to this principle mainly focus on: the vague and broad definition of terrorism; vague and open-ended terrorism-related legislation; and vague and uncertain criteria for measuring the severity of penalty.

4.4.3 The Principle of Legality (Nullum crimen sine lege, nulla poena sine lege)

Nullum crimen sine lege ("no crime without law") and nulla poena sine lege ("no punishment without law") is among the most important principles in criminal law, universally upheld in all major legal systems under the rule of law. This principle is sometimes known as the principle of legality. However, the connotations of the principle of legality are so wide-ranging that 'it is preferable to divide it into three distinct principles—the principle of non-retroactivity; the principle of maximum certainty; and the principle of strict construction of penal statutes.' 435

The core of this principle is that a person should never be convicted or punished of any criminal offence unless there are previously declared offences governing the

434 The details could be found in Chapter 5.
conduct in question.\textsuperscript{436} It not only excludes penalties for acts that are not prohibited by law, but also prohibits the application of \textit{ex post facto} or retroactive legislation. Under international human rights law, “no punishment without law” is a fundamental human right.\textsuperscript{437} The establishment of \textit{nullum crimen, nulla poena sine lege} promoted the rule of law under the Chinese Criminal Law by introducing more stability, predictability and openness into the law.

According to Ashworth and Horder, the non-retroactivity principle is also known as a basic legal principle: ‘No man is punishable or can lawfully be made to suffer in body or goods except for distinct breach of law established in the ordinary legal manner before the ordinary courts of the land’.\textsuperscript{438} When the Chinese Criminal Law introduced the \textit{nullum crimen sine lege and nulla poena sine lege} in 1997, it meant retroactivity was eschewed. According to Hall, \textit{nullum crimen sine lege} and \textit{nulla poena sine lege} and non-retroactivity are essential to the principle of legality in penal law in Western society. Wei Luo asserted that this was a positive change, noting: ‘this principle is conducive to avoiding inappropriate penalties, using different criteria, which result in imposing light punishment for serious crimes or severe punishment for minor crimes.’\textsuperscript{439}

4.4.4 The Principle of Minimal Criminalisation

The principle requires that the criminal proceedings should be used as a last resort.\textsuperscript{440} This principle provides that ‘although a state can decide to criminalise almost anything, it needs an extraordinary rationale to enact a criminal provision, which directly relates to fundamental rights and liberties.’\textsuperscript{441} According to Andrew Ashworth, when deciding whether to criminalise new offences, the following factors need to be considered:

\begin{itemize}
  \item \textsuperscript{436} The non-retroactivity principle does not affect the creation of defences to crimes, although the courts have sometimes deferred to the legislature on this matter. For theoretical discussion of this point, see PH Robinson, ‘Rule of Conduct and Principles of Adjudication’ (1990) 57 UCLR 729, and P Alldridge, ‘Rules for Courts and Rules for Citizens’ (1990) 10 OJLS 487.
  \item \textsuperscript{437} ICCPR, Art.15. It is noteworthy that the right cannot be restricted, even in times of emergency threatening the life of the nation: see Art 4(2) ICCPR.
  \item \textsuperscript{438} A Ashworth and J Horder, \textit{Principles of Criminal Law} (7\textsuperscript{th} edn, Oxford University Press 2013) 57.
  \item \textsuperscript{439} Wei Luo, \textit{The 1997 Criminal Code of PRC} (Hein 1998 ) 9.
  \item \textsuperscript{440} D Husak ‘The Criminal Law as Last Resort’ (2004) 24(2) OJLS 207-235.
  \item \textsuperscript{441} Ibid; Isra Samandecha, The Offences Relating to Terrorism in Thailand (Phd thesis, The University of Leeds, 2018) 122.
\end{itemize}
First, the behavior in question is sufficiently serious to warrant intervention by criminal law. Second, the mischief could be dealt with under existing legislation or by using other remedies. Third, the proposed offence is enforceable in practice. Fourth, the proposed offence is tightly-drawn and legally sound. Lastly, the proposed penalty is commensurate with the seriousness of the offence. 442

Ian Ayres and John Braithwaite have established the “Pyramid of Strategies of Responsive Regulation”443 which is presented below.

Figure 4.3: Pyramid of Strategies of Responsive Regulation

According to this chart, in the context of combating cyberterrorism, even though a state can take various measures to ensure national security and social stability, a criminal penalty shall be applied when only necessary. However, this principle of minimal criminalisation has not been properly applied in China. It can be seen that criminal law seems to be the first port of call when dealing with terrorism in practice.444 Even in cases that are not directly related to imminent security threats, the Chinese criminal justice system will bow to the overwhelming imperative of contributing to the now

---

443 I Ayres and J Braithwaite, Responsive Regulation: Transcending the Deregulation Debate (Oxford University Press) 16-22.
444 See Chapter 5 about existing provisions to combat terrorism in criminal law.
apparently perpetual “People’s War on Terror” with harsh and swift conviction.

China relies excessively on the use of criminal law to combat cyber terrorism without other strategies being sufficiently considered or applied alongside. In this regard, reference shall be made to E&W’s CONTEST strategy in particular to strands of ‘Prevent’ and ‘Protect’. In this regard, E&W’s approach would represent a good reflection of the policy of minimal criminalisation as discussed earlier, and shows that there are other ways apart from criminal law to apply counter-terrorism strategies. As for the principle of minimal criminalisation, some of the following main challenges are unaddressed: criminalisation of a wide range of terrorism precursor offences; early intervention; and the extension of criminal liability for terrorism-related offences.

4.5 Conclusion

This thesis aims to figure out whether ‘bourgeois liberalisation’ in E&W or ‘socialist law with Chinese characteristics’ produces markedly different legal responses to emerging global uncertainties such as cyberterrorism. For this purpose, it is relevant to map out the basic distinctive characteristics of the Chinese legal system. After a review of this system and its distinctly Chinese characteristics, the key salient feature is the legal reality of “rule by law,” which means the CCP is the ultimate authority and there is a lack of separation of powers, a lack of judicial independence, and a different understanding of human rights protection. This leads to the following possible solutions.

445 It is a criminal justice campaign that is fashioned along the lines of the so-called “strike hard campaigns” of the Deng Xiaoping era and requires the authorities to exercise their duties of criminal prosecution with utmost swiftness and render the harshest possible judgements.

446 For example, Hu Bo Case: Hu Bo posted his tweet about the ongoing riots in China’s far western region of Yarkand Country, and he was in trouble not only because he had repeated the official news, but he apparently had added some unconfirmed rumors about the intensity and extent of the riots. He was eventually sentenced to 6 months imprisonment. The court argued that his tweet had incited ethnic hatred and discrimination, which was considered his form of severely disrupting the social order, even through his lawyer asserted his clients did not even hint at the ethnicity of the rioters in Yarkand. See Daniel Sprick, ‘China’s Constitution and People’s War on Terror’ [accessed 23 Oct 2020].

447 Home Office, CONTEST, the United Kingdom’s Strategy for Countering Terrorism: Annual Report for 2015 (Cm 9310, 2016) 15-21; See also Counter-Terrorism and Security Act 2015, Section 26. Key objectives under ‘Prevent’ are to respond to the ideology of extremism and the threats, to prevent people from being drawn into terrorism and ensure that they are given suitable advice and support, and to work with specific sectors where there are risks of radicalization which need to address. Next, objectives under ‘Protect’ are to strengthen broader security, to reduce the vulnerability of transport network, to increase the resilience of critical infrastructure, to improve protective security for crowded places and people at specific risk from terrorism and improve security in key oversea locations.
implications in the legal responses to cyberterrorism: lack of counterbalance between security and human rights protection; violation of principles of certainty, proportionality, and minimal criminalisation; and a lack of due process and effective judicial review, thus enabling arbitrariness.

Therefore, we must consider whether these fundamental differences are actually important in shaping legal responses to global problems like cyberterrorism or whether legal systems as contrasting as those found in China and E&W are actually producing similar kinds of legal responses (for instance, vagueness, arbitrariness, and lack of counterbalance) to global uncertainties, like cyberterrorism. If they are important, we must then consider what this tells us about the causes of law-making in this field (if not fundamental legal principles and legal systems). All of these issues are investigated in subsequent chapters.
Chapter 5 The Legal Response to Cyberterrorism in China

5.1 Introduction

It will be recalled that China does not have a special counter-cyberterrorism law, but relies, instead, on existing Criminal Law (and its Amendments), Counter-Terrorism law and Cybersecurity law (CSL) to deal with cyberterrorism. Similar to E&W, using existing anti-terrorism legislation to counter the emerging threat of cyberterrorism presents a series of problems which the Chinese government has been struggling to deal with. This chapter attempts to comprehensively analyse and critically evaluate these laws in light of the basic principles elaborated upon in the last chapter. The purpose here is to figure out the main characteristics of the legal responses to cyberterrorism in China, and then compare these to the jurisdiction of E&W.

This chapter tackles six main issues. Firstly, this chapter commences with a consideration of China’s counter-terrorism strategy with particular regard to its preventive and pre-emptive tendency. Referring to the speech made by Xi Jinping on 26 April 2014 and the Overall Security Outlook, the guiding principle of counterterrorism highlights the Chinese state’s concern about collective interests, reflecting its quest for social stability and national unity. Furthermore, anti-terrorism laws and corresponding enforcement demonstrate the priority afforded by China to national security and social stability over the protection of individual human rights.

Secondly, there is no specific definition of “cyberterrorism” in China’s counterterrorism legislation, and it instead relies on the existing definition of “terrorism” in the CTL. It is arguable that this definition is too broad and vague, which may raise some problems with the designation of terrorism and terrorism-related offences. Moreover, an open-ended definition of terrorism may contravene the principle of certainty, resulting in arbitrariness.

Thirdly, for the purpose of the prevention of cyberterrorism, China has criminalised a wide range of terrorism-related precursor offences, which has involved taking the following steps:
(1) Intensification of crackdowns on association with, or the mere membership of, proscribed organizations;
(2) Suppression of financial assistance or other tangible support for terrorism;
(3) Criminalisation of the publishing of statements likely to be understood as direct or indirect encouragement of, or other inducement to, commit, prepare or instigate acts of terrorism;
(4) Criminalisation of a broad scope of preparatory acts; and
(5) Enforcing the overly broad offence of collection of information or possession of items for terrorism purposes.

Fourthly, China's counterterrorism legal framework still relies on a punitive strategy as per the in post-9/11 era. China appears to lean toward the toward intensification of laws and punishments on terrorism. Indeed, “terrorism connection” is an aggregate factor of penalty, and the maximum sentence for which is the death penalty. Moreover, the vague and uncertain criteria for measuring the severity of the penalty to be applied in such cases may violate the principles of certainty, proportionality and minimal criminalisation.

Fifthly, China has granted its executive organs broad discretion to designate proscribed terrorist organisations, which may contravene the presumption of innocence. Although the China's revised CTL has empowered the judiciary to designate terrorist individuals and organisations, thus arousing some concern with respect to due process and procedural justice, it still heavily relies on the executive department for designation, without independent review or a supervision system, which may leave the door open for an abuse of powers.

Finally, the enforcement of anti-terrorism legislation in China is increasingly focused on prevention rather than retribution. This implies that the vast majority of anti-terrorism laws can be seen as a gradual extension of the executive power to interrogate, detain, and control suspected terrorists during the pre-trail period. However, there are limited safeguards with respect to the suspect's rights in terrorism-related cases in China. In addition, there is a tendency to use non-criminal disruption methods to deal with
terrorism-related precursor offences in China.

5.2 Prevention and Pre-emptive Tendency

China's general strategy for countering terrorism encompasses not only ex-post approaches to terrorism, which focus on generating the effects of deterrence and denunciation, but also ex-ante responses to combating terrorism, which aim to disrupt and prevent terrorism.\(^{448}\) Similarly, E&W has also shifted towards the use of pre-emptive counter-terrorism strategies as a cornerstone of its counter-terrorism policy.\(^{449}\) In E&W, a national counter-terrorism strategy called CONTEST has been established around the themes of “Prevent, Pursue, Protect, Prepare.”\(^{450}\) This strategy entails the detection and investigation of threats at the earliest possible stage to disrupt terrorist activities before they can endanger the public.\(^{451}\) This preventive tendency could be analysed from the following substantive, political and practical perspectives.

(1) From a substantive law perspective, China has tended toward a preventive anti-terrorism legal framework, typified by the Chinese government’s move to criminalise an array of new terrorism offences and intensifying the sentencing and punishment of perpetrators.\(^{452}\) Furthermore, in China's counter-terrorism law reforms, the preventive rationale is articulated in the CTL, which states that ‘counter-terrorism efforts adhere to the principles of combining specialized efforts with the mass line, emphasizing prevention, combining punishment and prevention and anticipating the enemy's moves, and remaining proactive.’\(^{453}\) Depicted as a "preventive law" in tandem with the CL that punishes those who have committed terrorism offences, the CTL has developed a pre-emptive framework to identify, manage and control the threat that terrorism


\(^{450}\) C Heath-Kelly, 'Counter-terrorism and the Counterfactual: Producing the Radicalization: Discourse and the UK Prevent Strategy' (2013)15 (3) BJPIR 394, 395. The 'PREVENT' strategy is a set of British counter-terrorism initiatives, a stand of the 'CONTEST' strategy, first introduced in 2003 and revised several times over the last decade. The strategy is comprised of four work streams, known as prevent, pursue, protect, and prepare. Kent Roach and others, 'Introduction' in V Ramraj and others(eds), Global Anti-Terrorism Law and Policy (2nd edn, Cambridge University Press 2005).

\(^{451}\) Ibid.

\(^{452}\) The details could be found in following section 5.5.

\(^{453}\) China’s Counter Terrorism Law(CTL), Art.5.
represents.\textsuperscript{454} Compared to the CL, which criminalises preparatory offences, the CTL goes further by punishing grassroots organisations and civilians who have responsibilities to cooperate with the authorities to prevent acts of terrorism. To pre-empt terrorism in a high-tech era, telecommunication service operators, internet service providers (ISPs) and other institutions in China are now required to ‘provide technical interfaces, decryption and other technical support, and assistance to public security organs and state security organs undertaking investigation of terrorist acts in accordance with the law.’\textsuperscript{455} Pursuant to Art.19 of CTL, ISPs are further required to ‘put into practice network security systems and information content monitoring systems, technical prevention and safety measures, to avoid the dissemination of information with terrorist or extremist content.’\textsuperscript{456} By the same token, ISPs as well as telecommunications, finance, accommodation and car rental industries are obliged to undertake ID checks on clients.\textsuperscript{457} According to Art. 84 of the CTL, if a company does not comply with its legal obligations, it can be heavily fined or may even face up to 15 days of administrative detention.\textsuperscript{458} In a speech at the Telephone and Television Conference with the National Counter-terrorism Leading Group in January 2016, the Secretary of the Central Political and Legal Committee, Guo Shengkun, reiterated the importance of proactive policing and pre-emption in China’s counter-terrorism legal arsenal.\textsuperscript{459}

(2) From the policy perspective, the guiding principle of counterterrorism in China is also demonstrated in its prevention strategy. For example, Xi Jinping’s speech at the 14th Collective Study Sessions (26 April 2014) of the Politburo set the tone for the CCP’s position on counter-terrorism. The use of terms “decisive action,” “high level of pressure” and “resolutely” in the following passage clearly demonstrates the


\textsuperscript{455} CTL, Art.18, 85-93.

\textsuperscript{456} CTL, Art.19.


\textsuperscript{458} CTL, Art. 84.

determination of the CCP to fight terrorism and maintaining stability:

The fight against terrorism is a matter of state security, a matter of the vital interests of the people, a matter that concerns the overall situation of the stability of reform and development; it is a fight to maintain national unity, social stability, and people’s wellbeing. [We] must take decisive action, maintain a high level of pressure, and resolutely crush the arrogance of terrorists.460

This quote framed terrorism as an existential threat to state security, and highlighted that what the State is most concerned about is collective interests (“overall situation of the stability of reform and development”), reflecting its quest for legitimacy and its emphasis on national unity, and calling for extraordinary measures (“resolutely crush”).461 Xi Jinping’s speech as a guiding principle of counterterrorism also runs through China’s anti-terrorism legal framework. For instance, anti-terrorism legislation and enforcement also reflect this guiding principle, such as an overly broad and vague definition of terrorism, over-criminalisation, harsh punishment for terrorism and expansion of executive powers. All of these steps will be discussed in the following sections.

In addition, Xi Jinping proposed the Overall Security Outlook462 at the first meeting of the National Security Commission in April 2014, which became the guiding principle of China’s counter-terrorism strategy and legislation.463 Xi Jinping also pointed out, at the first Internet conference in April 2018, that ‘without cyber security, there would be no national security.’464 This implies that the CCP has incorporated the prevention and

---

462 Overall Security Outlook(综合安全观, zonghe anquan guan) includes: external security, internal security, security of national territory, citizen’s security, traditional and non-traditional security, development and stability.
control of cyberterrorism into the overall national security system.\textsuperscript{465} Due to their self-alignment with the CCP’s counter-terrorism principle, many Chinese scholars have justified the rationale behind preventive anti-terrorism laws and practices.\textsuperscript{466} Zhang Lei \textit{et al} claimed that under the guiding principle of the Overall Security Outlook, it is justifiable to apply preventive and punitive legislation and to expand the scope of criminal law to curb the risk of cyberterrorism.\textsuperscript{467} For example, compared to E&W, the CCP has adopted stricter policies to regulate the use of the Internet and block content that may destabilise the regime, which is particularly evident from the introduction of the so called Great Firewall and the concept of “cyber sovereignty.”\textsuperscript{468} Importantly, the CCP completely shut down access to the Internet after the Urumqi riots in Xinjiang in 2009. Although access restrictions have since been loosened, there are still many high-pressure measures applied to prevent the dissemination of “terrorist” ideology, such as the local government’s publishing of the Notice on Prohibiting the Dissemination of Terrorist Audio and Video in 2016.\textsuperscript{469} Guo Shengkun, the then head of the National Counterterrorism Leading Organ, proposed the criminal policy of “fighting against terrorism from an early stage” in August 2013, so as to prevent and


From a practical perspective, the enforcement of anti-terrorism legislations in China has increasingly focused on prevention rather than retribution.\footnote{The details could be found in following Section 5.9.} In particular, the executive organs are granted broad powers to interrogate, detain and control suspected terrorists during the pre-trial period. Furthermore, there is a tendency to use non-criminal disruption methods to deal with terrorism preparatory offences. In addition, according to the newly-published white paper and report from the SPC, the CCP placed emphasis on “striking at terrorism and extremism in accordance with the law”
and “giving top priority to a preventive counter-terrorism approach.” This implies that the courts in China also focus on prevention, which may contravene the principle of the presumption of innocence and a fair trial.

5.3 National Security and Social Stability Priority over Human Rights Protection in the Anti-terrorism Laws and Enforcement

There is a general paradox in the context of combating terrorism: on the one hand, terrorism poses a threat to the basic rights of citizens (such as the right to life); on the other hand, in a country’s efforts to thwart terrorism, it may erode civil rights to a certain extent (such as freedom of speech and privacy). Therefore, both China and E&W have to face the challenge of striking a suitable balance between security and liberty (two seemingly opposing interests) in their handling of cyberterrorism. Some previous Western studies have outlined that security and freedom should be balanced, especially as the threat of terrorism intensifies, and that some degree of freedom should be sacrificed in order to strengthen security. Meanwhile, the security-liberty balance has not stimulated much debate in China, which applies rule by law and therefore has the discretion needed to combat terrorism in an effective, albeit repressive, manner. We have observed how anti-terrorism legislation and enforcement in China have shown a growing tendency to ignore human rights, putting security first.

(1) Anti-terrorism legislation in China stipulates that public safety is the first priority. For example, according to Art. 1 of the CTL, the spirit of the CTL is to maintain national security and social stability. Moreover, Art. 5 of the CTL stipulates that "anti-terrorism work adheres to the principle of 'priority of precaution, combining punishment and prevention, maintaining pre-emption,' which establishes the "priority of security

476 CTL, Art.1.
and prevention” strategy to counter terrorism.” In addition, the purpose of revision of anti-terrorism clauses in Amendments of Criminal Law is also to severely combat terrorism offences, maintain national security and social order, and protect people's lives and property.

(2) In judicial practice, the guidelines of supreme judicial organs and supreme executive organs also emphasises the priority of security. For example, the reports of the SPC and Supreme People's Procuratorate (SPP) point out, ‘put the maintenance of national political security, especially regime security, and system security in the first place, and earnestly safeguard national security and social stability.’ According to this logic, it is easy to understand why counter-cyberterrorism legislation requires ISPs to provide a substantial level of individual data under some circumstances.

China has tried to make certain efforts to protect human rights at the legislative level. Art. 6 of the CTL stipulates that counter-terrorism work should be carried out in accordance with the law, should respect and protect human rights, and should safeguard the legitimate rights and interests of citizens and organisations, but without further explanation of how to achieve these goals. Therefore, in China, although policy slogans and legal provisions emphasise the protection of human rights, it is mere rhetoric. Some Chinese scholars have critically opined that legal responses and policy in relation to cyberterrorism are overreactive, which may curtail human rights, and that China should thus take into greater consideration the finding of a balance between security and liberty.

---

480 CTL, Art.19.
482 CTL, Art.6.
483 Qin Guanying, Research on Terrorism Crime from the Perspective of Non-traditional Security(非传统
In light of this, many human rights organisations or Western countries have expressed strong concerns or even condemnation regarding China’s human rights violations arising from its anti-terrorism laws. For example, the US State Department spokesman Mark Toner said at a regular press conference on 28 December 2015 that ‘the US remains concerned about the broad and empty wording of this legal provision and its definition, which may lead to further restrictions on Chinese speech, acceptance, peaceful assembly and religious freedom.’484 Freedom House also claims that China’s anti-terrorism laws represented another move to limit speech and dissent in the name of counter-terrorism, and that ‘the new anti-terrorism law has expanded the already extensive power of the Chinese government to monitor citizens, tighten censorship, and give officials legitimate excuses to detain journalists, activists and ethnic minorities and minority religious groups.’485 In addition, Amnesty International conveyed a similar view: ‘China’s anti-terrorism law is actually a law that violates freedom. It provides a huge space for China’s official repression activities, which will help the Chinese government safeguard national security, that is, defend the rule of the CCP.’486 In addition, some Western countries have expressed strong resistance to China’s new cyber security rules due to their worries their worries with regard to customer privacy and national security.487 Nicholas Bequelin argued that rules would give the Chinese government enormous power to monitor a substantial electronic database of telecom operators operating in China and force companies to provide decryption technology.488

485 Ibid.
In summary, China has come under international criticism for its alleged human rights violations.  

In response to the criticism that China’s counter-terrorism law amounted to human rights violations from the West and NGOs, the official response in China has been to accuse the West of “double standards.” For instance, the official Chinese media outlet, the People’s Daily, accused Human Rights Watch (HRW) of ignoring China’s specific realities and challenges, and blindly adopting self-righteous human rights standards to attack China. Moreover, the Chinese authorities have also claimed that its anti-terrorism laws were formulated with reference to Western anti-terrorism laws (such as those of the US) to defend its legitimacy. For example, Li Shouwei insisted that some of the assistance obligations imposed on ISPs were clearly defined in the law, and would not be used to infringe on the intellectual property rights of enterprises, or to undermine citizens’ freedom of speech and religious beliefs. In addition, similar to China, the US government also monitors Internet companies and requires them to disclose user data when investigating terrorism cases. Li Shouwei told Reuters reporters that Art. 18 was in line with the requirements of the UN Security Council on combating cyberterrorism, which are basically consistent with the legal provisions of European states and the US and meet the actual requirements of anti-terrorism work in China.

---

494 The NPC Law Committee interprets the Counter-terrorism law: Article 18 will not harm the freedom of speech of citizens on the Internet (People’s Net, 27 Dec 2015)
However, Teng Biao, a well-known former human rights lawyer and a visiting scholar at Harvard University, said that even if the Chinese anti-terrorism laws were literally completely consistent with the relevant laws of Western democratic countries, their implementation would be completely different due to stark differences in their legal systems and institutional environment. He also added:

In short, in the Western countries it has an independent judicial system, which has mutual supervision of power, including political party competition and independent news media for supervision. Therefore, for the purpose of counter-terrorism, the restrictions and monitoring of (Western government) citizen information do not lead to serious consequences.\(^{495}\)

Nicolas Bequelin, head of East Asia district at Amnesty International, expressed similar views on 27 December 2015, even though China’s anti-terrorism law is identical to the US anti-terrorism law, the implementation effect is also different due to the framework for law enforcement is different, and noting that:

In the West, even in the field of counter-terrorism, there will be opposition parties and human rights organizations that warn the government of ultra vires, but in China, no system or institution can guarantee that the government will not use this personal information as the tools of political suppression and further monitored journalists and activists.\(^{496}\)

Ultimately, these scholars hold that legal systems, to a large extent, shape China’s legal responses to terrorism. However, as revealed by further analysis in this thesis, E&W’s legal responses to cyberterrorism have been increasingly inclined to give priority to security.\(^{497}\)


\(^{496}\) Ibid.

\(^{497}\) The details could be found in Chapter 7.
5.4 Broad and Vague Definition of Terrorism

Like E&W, China does not have a specific anti-cyberterrorism law, and instead applies existing counterterrorism legislation to combat it. The main pieces of legislation which are applied to deal with cyberterrorism include: the Criminal Law (CL) and the CL Amendment (III), CL Amendment (VIII), and CL Amendment (IX) which criminalise a broad scope of terrorism-related offences; and the enactment of the Counter Terrorism Law (CTL) which provides a general legal basis for state laws to combat terrorism; and judicial interpretations regarding concerning cyberterrorism activities. The amendments in particular reflect an international tendency to expand the definition of acts of “terrorism” and to increase punitive measures.

(1) At present, there is no definition of “cyberterrorism” in Chinese legislation, but the Counter-Terrorism Law (CTL) does provide a definition of “terrorism.” It is arguable that this definition is too broad and vague, which may raise some problems with the designation of terrorism and terrorism-related offences. Firstly, it criminalises

498 In response to the UN Resolution 1373, the Standing Committee of National People’s Congress adopted and promulgated the “Criminal Law Amendment (III)” on 29 December, 2001, firstly proposed the term of “offence of terrorist activities”.


500 On August 29, 2015, the Criminal Law Amendment (IX) of the People's Republic of China (hereinafter referred to as the "Criminal Law Amendment (IX)") was issued by Standing Committee of National People's Congress (NPCSC), and came into force on Nov 1, 2015. Amendment(IX) of criminal law <http://www.lawinfochina.com/display.aspx?id=19864&lib=law> accessed 6 June 2017.

501 The Counter-Terrorism Law (CTL) as adopted at the 18th Session of the Standing Committee of the Twelfth National People's Congress of the People's Republic of China on December 27, 2015, was issued, and came into force on January 1, 2016.

502 For example, the offenders using Internet or social media incitement or propaganda terrorism could be seen as terrorism. See Opinions of the Supreme People’s Court, the Supreme People’s Procuratorate and the Ministry of Public Security on Several Issues concerning the Application of Law in the Handling of Criminal Cases Involving Violent Terrorism and Religious Extremism 2018 (2018 最高人民法院、最高人民检察院、公安部关于办理暴力恐怖和宗教极端刑事案件适用法律若干问题的意见) <http://en.pkulaw.cn.eresources.law.harvard.edu/> accessed 26 June 2018.


504 According to the Art. 3 of CTL, the definition of “terrorism” is “any proposition or activity that, by means of violence, sabotage or threat, generates social panic, undermines public security, infringes upon personal and property rights, or menaces state authorities and international organizations, with the aim to realize political, ideological and other purposes.” Article 3 of Counterterrorism Law, (Chinese: 中华人民共和国反恐怖主义法) <http://www.lawinfochina.com/Display.aspx?lib=law&Cgid=261788> accessed 5 June 2019.
“proposition,” which is difficult to clarify and may thus contravene the principle of certainty and legality. In the Chinese context, it means “expressing of opinions or speech,” which violates the constitutional freedom of speech.\textsuperscript{505} This implies that those who express their sympathy for terrorism on the Internet may potentially be designated as engaging in terrorism and be subject to criminal action accordingly. This also reflects the CCP’s combating of “behavioural terrorism” and “expression terrorism” in the same rigorous manner without distinction.

International Federation for Human Rights have contended that these stipulations are opaque and broad enough to justify the penalisation of ‘almost any peaceful expression of ethnic identity, acts of non-violent dissent, or criticism of ethnic or religious policies.’\textsuperscript{506} Human Rights Watch critically asserted that ‘the definition of what constitutes ‘terrorism’ is dangerously vague and open-ended, which could potentially apply to anyone advocating for policy changes, peaceful dissenters and critics of government or Party policies.’\textsuperscript{507} It also tautologically refers to “other terrorist activities,” potentially allowing any activity to be deemed a terrorist offense.\textsuperscript{508} Liu Yanhong meanwhile deemed that this broad and vague definition of terrorism may cause arbitrary interpretation in judicial practice, which may violate the principle of certainty and legality.\textsuperscript{509}

Moreover, the ever-expanding scope of the CTL and the CL is likely to make terrorism a “pocket crime(口袋罪),” \textsuperscript{510} thereby allowing law enforcement agencies to mark

\begin{itemize}
\item \textsuperscript{505} Article 35 of the Chinese Constitution regarding freedom of speech.
\item \textsuperscript{508} Ibid.
\item \textsuperscript{510} A “pocket crime” is an unofficial legal term that describes the vague definition of an offence that blurs the boundary between different offences. Drawing an analogy between an offence and a pocket crime, the phrase refers to such a definition of an offence that can be used to label more than one kind of criminal
\end{itemize}
unrelated activities as terrorism. He Ronggong argued that this broad definition of terrorism may cause arbitrariness and abuses of power in judicial practice.\textsuperscript{511} Indeed, it is broad enough to allow the CCP to not only criminalise political opponents, but also strengthen its social control. Conjecture, namely the use of vague definitions and terms, is also one of the CCP’s tactics, making it more flexible in its fight against cyberterrorism.

(2) In addition, this definition of “terrorism” is often conflated with “separatism” and “extremism.”\textsuperscript{512} This means that sympathisers and those expressing opinions on separatism could be punished according to counter-terrorism law.\textsuperscript{513} In practice, it is difficult to draw clear boundaries between terrorism, extremism and separatism. A violent incident carried out by members of a separatist organisation in attempting to intimidate citizens and challenge the secular system of a state can be considered

\begin{itemize}
\item[] He Ronggong, ‘Reflection on “Preventive” Anti-terrorism Criminal Legislation (“预防性”反恐刑事立法思考)’ (2013) 3 Chinese Law 156.
\item[] Shanghai Cooperation Organization (Ministry of Foreign Affairs of the People’s Republic of China 2001) defines the “three forces” that are frequently used in China’s counter-terrorism discourse. “Three forces” refers to “Terrorism, extremism and separatism”.
\end{itemize}

Terrorism is defined as follows.
[an] act intended to cause death or serious bodily injury to a civilian, or any other person not taking an active part in the hostilities in a situation of armed conflict or to cause major damage to any material facility, as well as to organize, plan, aid and abet such act, when the purpose of such act, by its nature or context, is to intimidate a population, violate public security or to compel public authorities or an international organization to do or to abstain from doing any act, and prosecuted in accordance with the national laws of the Parties.

In comparison, the definition of separatism is more related to territorial integrity.
“separatism” means any act intended to violate territorial integrity of a State including by annexation of any part of its territory or to disintegrate a State, committed in a violent manner, as well as planning and preparing, and abetting such act, and subject to criminal prosecuting in accordance with the national laws of the Parties.

And extremism is defined as an act aimed at seizing or keeping power through the use of violence or changing violently the constitutional regime of a State, as well as a violent encroachment upon public security, including organization, for the above purposes, of illegal armed formations and participation in them, criminally prosecuted in conformity with the national laws of the Parties; Zhang Chi, ‘How does Chinese Communist Party Legitimise its Approach to Terrorism?’ (DPhil thesis, University of Leeds 2018) 151.

In 2015, a Uyghur was convicted of “inciting separatism” and was sentenced to fixed-term imprisonment of three years and deprived of their political rights for two years. He confessed that he had uploaded a map of China which did not include Xinjiang, Tibet, Inner Mongolia and Taiwan, to his Q-zone (a social networking website), implying that Xinjiang is an independent country. Although his conviction was based on the consideration of other evidence including pictures promoting jihadi, the criminalisation of uploading pictures containing separatist ideas at least indicates the level of intolerance to any form of separatism.

terrorism, separatism and extremism at the same time. This means that those who have close ties with designated “terrorist organisations” may be punishable by law.514 For example, some organisations have been designated as terrorist organisations by the Chinese government because of their alleged involvement in violent separatist/terrorist attacks in China, although some of these organisations are considered legal outside of China.515

In addition, Chinese political officials have on various occasions indicated that the Chinese government resolutely opposes all forms of terrorism.516 This implies that in the eyes of the CCP, both extremism and separatism belong to categories of terrorism and should be combated similarly. Human Rights Watch (HRW) has warned that this will result in human rights violations, by conflating peaceful advocates of independence with terrorists.517 Inserting ambiguity into the definition of terrorism is part of the CCP’s law-making strategy, with the intention to create room for the Chinese government to legitimately combat any forces deemed as threats to state sovereignty and political legitimacy.518

Some of the criticism about the broad and vague definition of terrorism in China has been fierce. Although this definition of terrorism has been narrowed down to some

514 Zhang Chi, ibid 153.
515 Groups such as the East Turkistan Education and Solidarity Association provide funding and training for Uyghur students overseas. As these groups are grouped under the “East Turkistan forces”, those who have been associated with them are also potentially subject to the terrorism designation in China. Zhang Chi, ibid 153; Su Liwei and Feng Jin, ‘Why Did the ‘East Turkistan’ Seek Sanctuary from Turkey’ (东突 为何把土耳其当庇护所) (Huan Qiu, 24 July 2013) <http://world.huanqiu.comDEPTH_REPORT/2013-07/4164947.html.> accessed 20 Oct 2020; Zhang Chi, ibid 153.
extent. Zhou argued that the revised definition is still vague and may lead to an expansive interpretation. Human rights activists have meanwhile added that it can be used to suppress dissidents and religious minorities. For example, Leibold commented that the issue of terrorism had been framed in China in the past to mainly target the Uyghurs, Tibetans and those who disagreed with official Chinese policies. Elsewhere, Bequelin argued that China’s claims about terrorism were highly politicised and included targeting of peaceful dissenters. Sophie Richardson, connected the vague interpretations of terrorism with Chinese government’s crackdown on peaceful dissent, as reflected in the doubling of prosecutions for state security and terrorism offences in 2015. Some human rights organisations have also criticized the implementation of the CTL, which has greatly deteriorated the human rights situation for some ethnic minorities (such as the Uyghurs) in China. Additionally, the broad definition of terrorism may have led to some divergence between the CCP and the

---

519 Liu Rong, ‘Second Amendment of the Anti-Terrorism Law: Clarify That Procedure to Cross-Examine, Inspect, and Summon Should Be Carried out According to Law(反恐法二次修改:明确盘问、检查、传唤需依法进行)’ (People net, 25 February 2015)<http://npc.people.com.cn/n/2015/0225/c14576-26595555.html.>accessed 20 Oct 2020. In the second draft apparent conflation of terrorism and separatism was also removed by deleting “create ethnic hatred, subvert the regime, and separate the country”. This is evident from the addition of “undermine public safety, infringe on personal and property rights” to the definition. The second revision was criticised by some members of the People’s Congress for omitting the political and ideological nature of terrorism, and the third draft thus stated that the aim of terrorism is to realise political, ideological objectives.


international community regarding the designation of terrorist organisations.\textsuperscript{526} For instance, the CCP has listed the World Uyghur Congress as a terrorist group\textsuperscript{527}, while in the eyes of the international community, this is a legal organisation that advocates human rights. The UN Office of the High Commissioner for Human Rights recognised it as an Uyghur representative group and has allowed it to actively participate in various forums of the UN Human Rights Council.\textsuperscript{528}

(3) At the same time, according to Art. 3b of the CTL, the scope of “terrorist activities” is very broad, including acts of instigation, preparation, assistance and implementation, meaning basically that the entire process of behaviour (from the planning stage to the implementation stage) has been identified as terrorism activities.\textsuperscript{529} Elsewhere, the term of “other terrorist activities” in this provision is considered as “pocket clause” which leaves the huge leeway for interpretation in judicial practice, and may cause violations of the principle of certainty.\textsuperscript{530} The vague definition of terrorism and broad boundaries of “terrorist activities” give rise to the vague and open-ended terrorism-related legislation. There are countless critical voices when it comes to the CL, the CTL and other terrorism-related legislation in China due to their vague and ambiguous
For instance, HRW asserted that ‘many aspects of the counterterrorism law are incompatible with international human rights law and could facilitate future human rights violations.’ In fact, using broad and vague language is a feature of most Chinese legislations.

(4) A further aspect to consider here is that the broad and vague definition of terrorism may allow for a certain degree of flexibility and arbitrariness in the designation of terrorist individuals and organisations. Moreover, the executive organs have been granted broad power with regard to the designation of terrorism, ranging from ad-hoc list-making to the “double track” system.

The Ministry of Public Security announced the first batch of designated list on 15 December 2003, which included four terrorist organisations and 11 individuals. Subsequently, the Ministry of Public Security announced the second list in 2008 and the third list in 2012. These lists are based on the Criminal Law, National Security Law (NSL) and its Rules for Implementation, and the international counter-terrorism conventions that China has ratified, including Resolution 1373. Zhao Yongchen, the then Vice-Director of the Ministry of Public Security, addressed some criteria of the

---


534 The “double track” system of designation (双轨制认定), the details could be found in following section 5.8 of this chapter; see also Zhang Chi (n 25) 158-161.

designated individuals.537 Afterwards, the Chinese government issued “red notices” on all of the 11 proscribed individuals in the first list. One controversial inclusion was that Dolkun Isa who was accused of theft, robbery and a series of bomb attacks in Khotan county, as well as propaganda, and supporting and participating in terrorist activities.538 However, he gained sympathy from some human rights organisations and Uyghur groups in the West.539 For instance, the World Uyghur Congress criticised China of lacking conclusive evidence to prove its allegations,540 while HRW accused China of abusing the “red notice” against political opponents.541 Indeed, Interpol revoked the “red notice” because of a lack of convincing evidence.542

These lists have increasingly tended to be used as a legal tool rather than a political document. For example, the third list provided for the freezing of assets of proscribed individuals. In addition, the second and third lists provided evidence of associations between proscribed individuals and terrorist organisations. This seemed to represent the CCP’s response to previous international accusations of a ‘lack of conclusive evidence.’543

However, many Chinese scholars have argued that it would be justifiable to expand the scope of anti-terrorism legislation and criminalise a wide range of precursor terrorism offences.544 Moreover, the close tie between Chinese authority and

537 These criteria include: association with association with, leading, organizing, participating in the proscribed terrorist groups; organising, planning, inciting, propagating or instigating terrorist activities; funding or training, supporting proscribed terrorist organisations and individuals. Zhao Yongchen, 2003. ‘Criteria for the Identification of Terrorist Organisations and Individuals(认定恐怖组织、恐怖分子的具体标准)’ (People net, 15 December 2003)< http://www.people.com.cn/GB/shehui/1060/2247177.html. >25 Sep 2020.
539 Zhang Chi, ibid 159.
544 Details could be found in Literature Review Chapter.
academia limits the amount of objective research on existing anti-terrorism legislation. For example, due to their self-alignment with the CCP line, many Chinese scholars have refrained from challenging the state definition of terrorism. Most scholars instead function to justify China’s counter-terrorism policies and legal responses. For example, some scholars argue that although inciting, preparing and assisting terrorism offences would not of themselves bear actual and urgent harm upon the public compared to the terrorist attacks, these terrorism activities would still pose certain risks to the public, and should thus be intervened in from an early stage.

5.5 Criminalisation of A Wide Range of Terrorism Precursor Offences

According to Clive Walker, the first function of criminal law is to allow for prescient intervention against terrorism endangerment and well before a terrorist crime is carried out. The more catastrophic the potential offence, the greater the imperative to prevent, and the more it can justly be said that prosecution and punishment of the already-completed act comes too late, and this is the rationale according to which many countries generally criminalise preparatory, assistance and association offences related to terrorism. However, Andrew Ashworth and Lucia Zander proposed that in order to curtail abuses of preventive counterterrorism provisions, it might be necessary to insist on adherence to the principles of necessity, least restrictive appropriate means, sufficient substantiating evidence, and a fair trial. China’s Criminal Law has criminalised a wide scope of terrorism precursor offences online and offline, which may raise concerns about possible violations of the principles of proportionality and minimal

546 Details could be found in Literature Review Chapter.
criminalisation.

The terrorism offences related to the criminal law’s precursor impact can also refer to the term “precursor crime”. “Precursor crime” refers to the criminalisation of acts in preparation of terrorism.551 Today, compared with traditional terrorism, cyberterrorism is difficult to prevent due to its anonymity and convenience.552 Traditional criminal law generally intervenes after, rather than before, a crime takes place,553 and in judicial practice, there are also some obstacles to early intervention regarding admissibility, disclosure, and proof.554 In order to combat cyberterrorism effectively, as the main mechanism to respond to these threats, the CL is utilised to prevent or avert the anticipatory risks of terrorism.555

As well as the broad and vague definition of terrorism, China has also criminalised a broad series of new terrorism-related offences, which could be applied to cyberterrorism. Since 2001, China has made several piecemeal amendments to its CL, CTL, Cyber Security Law and a number of administrative laws regarding the regulation of terrorism.556 A highlight of this reform has been the inclusion of the doctrine of pre-emption, which advocates the prevention and control of terrorist acts.557

Through introducing a series of terrorism offences from the preparatory stage to the committing stage, Chinese CL has taken an exceptional move by criminalising a wide scope of behaviours and imposed harsher penalties, while a number of specific laws and relevant administrative regulations558 have also been established, serving as an

---

554 Joint Committee on Human Rights, Counter-Terrorism Policy and Human Rights: Prosecution and Pre-Charge Detention (2005-06 HL 240, HC 1576) paras.12, 28.
558 For example: To be consistent with the Criminal Law, the Anti-Money Laundering Law characterizes the act that attempts to conceal or hide gains derived from terrorist crimes as money laundering and subjects it to administrative control and criminal punishment.
ancillary regulatory mechanism to regulate some more terrorism-related offences. These offences are criminalised at an early stage and carry formal criminal punishments including criminal detention, control, and fixed-term imprisonment. Their existence in the Criminal Law functions as a legitimate basis upon which the Chinese legal authorities are now able to pre-emptively control and monitor potentially dangerous individuals as they see fit. So, both China and E&W have demonstrated a similar tendency to expand criminalisation of terrorism offences, and the threshold of criminal liability has been shifted to an earlier stage of terrorism-related activity.

Many Chinese scholars justify the necessity and rationality of criminalising a wide range of terrorism precursor offences under the preventive strategy of counterterrorism. Additionally, some scholars have proposed that China should create a specific anti-cyberterrorism provision to clarify the definition and scope of cyberterrorism.

However, according to Andrew Ashworth, when deciding whether to criminalise new offences, it needs to be considered that the behaviour in question is sufficiently serious to warrant intervention by criminal law. Given this, a few Chinese scholars have critically claimed that the scope of terrorism precursor offences are too broad and allow for excessive pursuit of prevention and severe punishment, which may contravene the

principle of minimal criminalisation.\textsuperscript{564} Therefore, the precursor offences should be serious enough to be criminalised by criminal law in the context of combating cyberterrorism.

However, through a closer analysis of existing anti-cyberterrorism legislation, similar to the UK, the general criminal law principles may be partially or entirely ignored. First, the early intervention and extension of criminal liability violates the principle of minimal criminalisation. Second, the vagueness of these inchoate offences and lack of specific terms contravene the principle of legal certainty. Third, lack of proximity to the commission of the ultimate harm and the risk of harm result to harsh punishment may violate the principle of proportionality. This issue will be analysed in detail in the following sub-sections.

5.5.1 Intensification of the Crackdown on Association with or Membership of Proscribed Organisations

One frequently encountered type of expansion of precursor crime is criminalization of association with or the mere membership of proscribed organisations. Pertinently, Art.120 was inserted into the Criminal Law in 1997, which stipulated the offence of "organizing, leading, and participating in terrorist activities."\textsuperscript{565} According to this provision, as long as the perpetrators have organised, led, or participated in a terrorist organisation's activities, they will commit this offence regardless of whether or not they commit other crimes (such as murder, explosion, or kidnapping). Pi Yong expressed a positive attitude to this provision because it intervenes before an actual violent terrorist activity can occur, thus preventing the harmful consequences.\textsuperscript{566} As this provision


\textsuperscript{565} China’s Criminal Law, Art. 120 Para.1: “Whoever organizes, leads or actively participates in a terrorist organization shall be sentenced to a prison term ranging from 3 to 10 years; other participants shall be sentenced to a prison term less than 3 years, criminal detention or public surveillance.” Among them, the "organize terrorist organizations" refers to the act of convening of a number of people as the ringleader or any other principals to initiate, or recruit, employ, draw, and encourage many people establish terrorist organizations. "Leads terrorist organizations" refers to the person who has succumbed to the leadership of a terrorist organization, and has conducted planning, commanding, arrangement, and coordination of the establishment of terrorist organizations and terrorist activities after their establishment.

\textsuperscript{566} Pi Yong, Research on Legislations against Cyber-Terrorism(防控网络恐怖活动立法研究) (Law Press
does not stipulate a specific means of conduct, persons using the Internet to implement these acts are also punishable in accordance with this provision. Moreover, the term “other participants” alludes to “pocket crime,” which is overly broad and vague and could be applied to any activities (online or offline) in connection with a proscribed organisation.

Additionally, the Amendment (III) to Art.120 meanwhile suggests a turn not only towards the criminalisation of “terrorism” but also of political dissent in general. However, the failure to define what constitutes a “terrorist organisation” leaves the door open for this law to be deployed against any groups, organisations or religious associations that the State deems to be a threat, whether they be political, non-political or non-violent. Basically, this provision may violate the principles of certainty and minimal criminalisation.

5.5.2 Suppressing Financial Assistance or other Tangible Support for Terrorism

Another type of extended anti-terrorism precursor offence is criminalization of the financing of terrorism. Various social media platforms and online financial tools (such as QQ, WeChat, and PayPal) are easily used by terrorists to raise funds for their activities. Additionally, the UN Resolution 1373 requires all member states to ensure that terrorism financing is treated as a serious crime.

In order to deal with online fundraising and in response to this Resolution, the CL was further expanded to incorporate the offence of financing terrorism by holding both individuals and units

\[\text{References}\]

567 A “pocket crime” is an unofficial legal term that describes the vague definition of an offence that blurs the boundary between different offences. Drawing an analogy between an offence and a pocket crime, the phrase refers to such a definition of an offence that can be used to label more than one kind of criminal activity, just like a pocket that contains more than one items. Zhang Xun, ‘Research on the Crime of Picking Quarrels and Provoking Troubles, from the Perspective of Pocket Crime’ (2013) 3 Politics and Law; Zhang Chi, ‘How does Chinese Communist Party Legitimise its Approach to Terrorism?’ (DPhil thesis, University of Leeds 2018) 165.

568 China’s Criminal Law, Art. 120a: “Whoever provides funds to any terrorist organization or individual who engages in terrorism shall be sentenced to fixed-term imprisonment of not more than five years, criminal detention, public surveillance or deprivation of political rights, and shall also be fined; if the circumstances are serious, he shall be sentenced to fixed-term imprisonment of not less than 5 years, and he shall also be fined or his property shall be confiscated.”


criminally liable for making funds, financial assets and economic resources available to those seeking to participate in terrorist acts.\textsuperscript{571}

Zhang Lei deemed that this provision should be further expanded to cover the offence of cyberterrorism fundraising.\textsuperscript{572} Moreover, some scholars have suggested that the executive powers should be further expanded in judicial practice, such as setting up the inversion of the burden of proof to reduce the prosecutor’s burden of proof \textsuperscript{573}, thereby allowing asset-freezing without a warrant or conviction to improve efficiency \textsuperscript{574}.

As evaluated by the Financial Action Task Force (FATF), Art. 120a is ‘a brief and sweepingly formulated provision’ on a complex offence and needs ‘further refining.’\textsuperscript{575} Firstly, the provision does not mention the raising of funds for the perpetrators themselves to pursue terrorist activities. According to the International Convention for Suppression of the Financing of Terrorism (1999), member states are required to criminalise the collection of financial resources for terrorism purposes as a stand-alone offence.\textsuperscript{576} So, as long as the perpetrator intends to raise funds to commit terrorist activities, they will be punished regardless of whether the funds have been handed over to terrorist individuals or organisations. Secondly, there is still no exact definition of the “financing of terrorism.” According to the literal meaning of the provision, “terrorism financing” means to ‘provide funds to any terrorist organization or terrorist individual.’ But dubiety persists with regard to how an individual or organisation can be designated as “terrorist” before financing a terrorist act.\textsuperscript{577}

\textsuperscript{571} China’s Criminal Law, Art. 120a.
\textsuperscript{575} Zhou Zunyou, \textit{Balancing Security and Liberty: Counter-Terrorism Legislation in Germany and China} (Dunker & Humbiot 2014) 141.
\textsuperscript{576} International Convention for Suppression of the Financing of Terrorism (1999).
5.5.3 Criminalisation of Publishing of Statements Likely to be Understood as Direct or Indirect Encouragement or other Inducement to Commit, Prepare or Instigate Acts of Terrorism

Criminalising the fabrication or dissemination of false terrorist information represents a further expansion of the precursor terrorist offences. Since the tightening of the CL, the dissemination of false information has become a stand-alone clause, and the standard of sentencing is determined according to the extent of disruption to social order. It should be pointed out that an important element of this offence is that the damage must be serious enough to disturb the social order. As the legislature explains, “the serious disturbance of social order”, as a significant constitutive element of the offence, refers to the social panic leading to the breakdown of daily social activities. Like a number of the previous articles, the Art. 291a also fails to specify a maximum sentence or to clearly define “serious consequences.”

The purpose of introducing this clause was to curb the spread of rumours or the dissemination of fabricated information related to terrorism. What started out as an attempt to discourage libellous vitriol on the Internet quickly became a powerful means through which the Chinese criminal justice system could control social media content. In 2013, the SPC had published three “model cases” for the adjudication of spreading false terrorist information, which represented a non-binding guide for lower courts.

---

578 China’s Criminal Law, Art. 291a: “Whoever spreads hoaxes of explosive, poisonous or radioactive substances, of infectious-disease pathogens or of other substances, fabricates terrorist information invoking explosive, biochemical, radioactive or other threats, or intentionally disseminates terrorist information while clearly knowing that it is fabricated, thereby seriously public order, shall be sentenced to fixed-term imprisonment of not more than five years, criminal detention or public surveillance; if the consequences are serious, he shall be sentenced to fixed-term imprisonment of not less than five years.”

579 Zhou Zunyou, Balancing Security and Liberty: Counter-Terrorism Legislation in Germany and China (Dunker & Humblot 2014) 145.

580 Case1: Zhang Wanqi fabricates false terrorism information case; Case 2: Pan Jun fabricates false terrorism information case; Case 3: Xiong Yi fabricates false terrorism information case (案例一：张琬奇编造虚假恐怖信息案；案例二：潘君编造虚假恐怖信息案；案例三：熊毅编造虚假恐怖信息案) see The Supreme People’s Court published 3 model cases regarding Fabricated Terror Threat (People net, 29 Sep 2013)<http://legal.people.com.cn/n/2013/0929/c188502-23074503.html> accessed 13 Nov 2020. The criminal law until 2015 would warrant a fixed term of imprisonment of up to five years for such conduct, hence the three model cases saw sentences between fifteen months and four years, depending mainly on the seriousness of the disruption of social order and on the underlying motive for disseminating the false information.
Human Rights Watch has argued that this provision does not clarify what constitutes a “rumour,” heightening concerns that the provision will be used to curtail freedom of speech, particularly on the Internet.\textsuperscript{581} Human Rights Watch has also claimed that Chinese activists are often prosecuted for speech-related “crimes”, such as “inciting ethnic hatred.”\textsuperscript{582} Sophie Richardson stated that this provision is a powerful weapon for the CCP to control online speech, including the sharing of any reporting of events that departs from the official version of events.\textsuperscript{583}

According to the Court spokesman Sun Jungong: ‘No country would consider the slander of other people as ‘freedom of speech.’’\textsuperscript{584} The CCP believes that rumours or false terrorism should not be protected by the freedom of speech prescribed by the Constitution. This means that in the eyes of the CCP, freedom of speech only protects those statements that the CCP deems to be legitimate. Therefore, the CCP has the authority to determine what speech is a rumour and what speech is not. Accordingly, this provision may have a so-called chilling effect on the online communities in China.

Moreover, some scholars have gone further by expanding the scope of this provision to cover the offences of recruiting cyberterrorists,\textsuperscript{585} inciting participation in a cyber terrorist organisation, shielding and condoning cyber terrorist activities and increasing the penalties for cyberterrorists.\textsuperscript{586}

\textbf{5.5.4 Criminalisation of Terrorist Propaganda and Incitement (Art. 120c)}\textsuperscript{587}

\begin{itemize}
\item \textsuperscript{582} For example, case of human rights lawyer Pu Zhiqiang, who has been detained since May 2014 for a number of social media posts questioning the government’s policies towards Uighurs and Tibetans.
\item \textsuperscript{584} Jonathan Kaiman, ‘China cracks down on social media with threat of jail for ‘online rumours’’ (\textit{the Guardian}, 10 Sep 2013) <\url{https://www.theguardian.com/world/2013/sep/10/china-social-media-jail-rumours} > accessed 21 September 2019.
\item \textsuperscript{585} Zhai Xiufeng, ‘The mobilization characteristics and dilemma of Cyberterrorism Countermeasures (网络恐怖主义的动员特征及应对困境)’ (2017) 39 Modern communication (Journal of Communication University of China) 160-162.
\item \textsuperscript{586} Zhang Lei, ‘A study of Prevention and Control on Cyberterrorism Crime from the Perspective of Overall National Security (总体国家安全观视角下网络恐怖主义犯罪防控研究)’ (DPhil thesis, Jilin University 2020)111-112.
\item \textsuperscript{587} China’s Criminal Law, Art. 120c: "Whoever advocates terrorism or extremism or instigates terrorist activities by way of preparing or distributing any books, audios or video materials or any other article advocating terrorism or extremism or by instructing or issuing information shall be sentenced to
The use of criminal law to regulate the incitement of terrorist activities, especially the indirect incitement of terrorist activities, is considered to be an important means of cracking down on terrorism at source. In 2005, Art. 1 (a) of UN Resolution 1624 (2005) stated that ‘all countries are called upon to take necessary and appropriate measures in accordance with their obligations under international law in order to legally prohibit incitement to commit one or more types of terror behavior.’ At first glance, Art. 120c (criminalising incitement to commit terrorism) is perfectly in line with international practice. However, there are some problems with Art. 120c.

Firstly, the terms of “extremism” and “terrorism” in this provision are not explicitly defined. The term “extremism” is frequently used in the CL, sometimes used in parallel with “terrorism” and sometimes used alone, but it does not clarify the difference between the two terms. The conflation of “terrorism” and “extremism” violates the principle of legality. More specifically, the open-ended scope of the term of “advocating terrorism” and the vague definition of "extremism" in this provision arouses concern since the State may misinterpret these terms to facilitate the execution of law enforcement activities against non-violent dissent.

Secondly, the offence of inciting terrorism is deliberately broad and vague, and this issue is analysed in three particular aspects below.

(A) With respect to the mens rea, Art. 120c does not explicitly stipulate whether incitement to terrorism requires a deliberate intention, but judicial practice shows that even when the perpetrator has no specific intention, they can also be convicted under this provision. A “model case” issued by the Supreme People’s Court is Zhang Xinghai’s advocating of terrorism and extremism online. In this case, the perpetrator

imprisonment of not more than five years, criminal detention, surveillance or deprivation of political rights in addition to a fine; or if the circumstances are serious, be sentenced to imprisonment of not less than five years in addition to a fine or forfeiture of property.”

588 UN Security Council, Resolution 1624 (14 Sep 2005), UN Doc S/RES/1624.
590 At the beginning of 2016, the defendant Zhang Xinghai went online to access QQ chat software and other applications through the mobile Internet for the purpose of curiosity or fun (attracting others’ attention and improving the number of views), and found that some people published violent horror
was convicted for ‘curiosity about terrorism related videos.’

According to the empirical research of Mei Chuanqiang and Yan Jinlei, as long as the perpetrators carried out propaganda and incitement acts, then regardless of whether they intended to incite terrorism or not, in judicial practice they would be punishable by Art. 120c. In fact, in some cases, the perpetrator did not have the special intention of inciting terrorism, but used the network to upload, download and forward terrorist videos and pictures for reasons such as curiosity, fun and attraction (such as the Zhang Xinghai case). It could be argued that the lack of special intention to incite terrorism would equate to over-criminalisation. Similarly, the issue of criminalising curiosity about terrorist offences also occurred in the UK, which may violate the principle of minimal criminalisation.

(B) In terms of actus reus, both China and E&W have adopted a wide scope of incitement, including direct incitement and indirect incitement. Pertinently, a comparison can be drawn here with the UK Terrorism Act 2006, Section 1 which refers to “direct and indirect encouragement of terrorism.” In addition, this provision does not explicitly stipulate the use of the Internet to carry out the incitement of terrorism and extremism, but according to judicial practice, individuals are punished for such videos and pictures on the Internet, and then downloaded and saved them. After that, he uploaded some of the violent video and pictures downloaded from it to the QQ space for others to watch. The above videos and pictures all involve the use of extremely bloody and cruel means to endanger the lives of others and promote religious extreme thoughts. They are typical violent terrorist propaganda. Finally, The defendant Zhang Xinghai committed a crime of terrorism and extremism, sentenced to two years and three months in prison and fined RMB 5,000.


593 ‘This Section applies to a statement that is likely to be understood by some or all of the members of the public to whom it is published as a direct or indirect encouragement or other inducement to them to the commission, preparation or instigation of acts of terrorism or Convention offences’.
conduct regardless of whether they intended to incite terrorism online or offline. In the case of Aini Aisan, the conduct penalised was watching and listening to violent terrorist videos and audio material, terrorist training, inciting attacks on patriotic believers, and assigning others to carry out terrorist attacks.

(C) In terms of probability of harm, the incitement of terrorism is an inchoate offence, whereby the incitement does not need to occur in practice, nor does it require the pursuit of harmful consequences. Art. 120c does not specify whether incitement needs to be made public or targeted toward an unspecified majority. Zhang and Zhao claimed that an incitement to terrorism should need to target the public. It could be argued that the provisions are too general and extensive, lacking in clear and detailed descriptions and constraints on crime elements, and are open to wide interpretation by judges. Moreover, the standard of "serious circumstances" and "particularly serious circumstances" needs to be clarified, or there may be overly extended application in judicial practice and thus over-criminalisation.

Xiang Huai held that judicial interpretation should set a clear standard for terrorism and extremism, to avoid excessive arbitrariness in practice and violation of the principle of legality. Du Xiaofei, meanwhile, stated that anti-terrorism legislation is suspected of being over-criminalised, which may lead to excessive state power and a human rights crisis. Furthermore, Liu Renwen proposed that although the serious harm inflicted by terrorism demands early intervention by law, the basic rights of citizens cannot be sacrificed in doing so. The principles of proportionality and legality should thus be fully

---

595 As of April 30, 2018, according to the data of China judgement online, there are in total of 21 cases convicted of this crime, without exception, all of which are committed by using the Internet.
597 The possibility of the risk of harmful consequences to the public.
600 See Li Zhe and Zhang Yi, ‘Comparison of inciting terrorism act in China and the UK’ (2016) 24(5) Journal of the National Prosecutor's College 49.
602 Xiaofei Du, ‘Research on Anti-terrorism Legislation in the UK’ (Master thesis, Shandong University 2011) 34
respected under the judicial process.  

5.5.5 Criminalisation of a Broad Scope of Preparatory Terrorist Acts (Art. 120b)

China has further expanded the scope of its CL by introducing some instigation, preparation and assistance offences under Amendment (IX). In addition, the crime of "financing terrorism activities" has been amended to "assisting terrorism activities" which serves to encompass various activities including training, recruiting and transporting. To avoid the occurrence of serious terrorist acts, these offences penalise suspects at a much earlier stage of planning than the ordinary criminal law of attempt. In particular, the revised CL and the CTL have classified preparatory offences in two categories that are subject to different sanctions according to the degree of "seriousness." While more "serious" preparatory offences amount to criminal penalties, less "serious" preparatory offences are subject to administrative punishment.

Wang has expressed agreement with such a preventive strategy to curb cyberterrorism at an early stage. However, Zhang Mingkai argued that the provisions relating to countering terrorism in Amendment (IX) in general are too broad and intervene too early to protect legal interests (法益), leading to over-criminalisation and excessive punishment. For instance, compared with the previous Art. 120 in the Criminal Law 1997, the revised Art. 120a added a property penalty for perpetrators. This demonstrates that China has been consistently increasing penalties to combat terrorist crimes.

605 China’s Criminal Law, Art. 120b and China’s Counter-Terrorism Law, Art.5.
606 Ibid.
609 China’s Criminal Law, Art.120a: “Any individual who provides financial support to a terrorist organization or conducts terrorist activities, or provides training on terrorist activities shall be sentenced to imprisonment of not more than five years, criminal detention, surveillance …; or if the circumstances are serious, be sentenced to imprisonment of not less than five years....”
The precursor terrorism-related offences can be found in the Art. 120b, such as the offence of preparing for the conducting of terrorist activities.\textsuperscript{610} It could be criticised and debated that Art. 120b is too ambiguous and broad, which might contravene the principles of certainty and minimal criminalisation. For instance, this article does not specify what constitutes "organizational training terrorism" and, moreover, the term of "any other intermediate acts" amounts to a "pocket clause", which may cover almost any acts related to terrorism. These offenses are related to inchoate offences. For instance, "engagement" with the planning or preparation of any terrorist activities is prosecuted at a much earlier stage than for instances of attempted crime. Likewise, the CTL has incorporated a list of similar offences with a lower degree of malice and subjected offenders to custodial administrative sanctions.\textsuperscript{611}

A comparison can be drawn here with the UK’s Terrorism Act 2006(TA 2006), s 5 which is considered a good reflection of the precursor objective.\textsuperscript{612} In addition, the term of “training” lacks clarity, particularly with regard to whether it covers moral training or is restricted only to physical training for terrorism purposes. In terms of training for terrorism, a comparison can be also made here with s 54 of the TA 2000 and s 6 of the TA 2006 which are seen as clear “precursor" offences regarding terrorism training.\textsuperscript{613} It can be seen that s 54 of the TA 2000 provides a clear description of training for terrorism, with specific examples of actions. This reflects the high standard in legality in dealing with broad “precursor offences." Thus, it has been stated by Kent Roach that s 54 of the TA 2000 is a good example of the expansionist tendencies of modern anti-terrorism law that deals with inchoate offences such as attempted conspiracy or remote connections with actual acts of terrorism.\textsuperscript{614} In contrast, Art. 120b of China’s Criminal Law lacks a clear definition, as previously

\textsuperscript{610} China’s Criminal Law Art.120b: "(1) Preparing lethal weapons, hazardous articles or other tools for conducting terrorist activities. (2) Organizing training on terrorist activities or actively participating in training on terrorist activities. (3) Contacting any overseas terrorist organization or person for the purpose of conducting terrorist activities.(4) Making a plan or any other preparation for conducting terrorist activities...."

\textsuperscript{611} China’s Counter-Terrorism Law, Art. 80 and Art.81.

\textsuperscript{612} Details will be found in Chapter 7.


discussed, and this may lead to several problems in the operations of enforcement organs.

Based on the investigation presented above, the relevant provision could be deemed vague and this may amount to a deficiency with respect to the principle of legality. As criminal law is directly related to the basic rights and liberties of the people, it must be clear and should not rely heavily upon a court’s interpretation.

5.5.6 Overly Broad Offence of Collection of Information or Possession of Items for Terrorism Purposes

Another precursor offence is the possession of any book, audio or video materials or any other items related to advocating terrorism or extremism (Art. 120f). According to data from China Online Judgement, from 2016 to present day there have been a total of 25 cases concerning the possession of terrorist and extremist articles. In all such cases, the perpetrators used use the Internet or social media to download or upload videos. This shows that terrorists are now more inclined than before to use the Internet to acquire or keep terrorism-related materials.

Similar to inciting terrorism, the conviction threshold for this crime is very low: as long as the perpetrator holds audio or video materials or other items related to terrorism, they are deemed to be committing an offence under this provision, regardless of any terrorism-related intention and the consequences of holding such materials.

Moreover, it is difficult to clarify the term “serious circumstances” which may lead to

---

615 China’s Criminal Law, Art. 120f: “Whoever illegally holds any book, audio or video materials or any other article while obviously aware that it advocates terrorism or extremism shall, if the circumstances are serious, be sentenced to imprisonment of no more than three years, criminal detention or surveillance in addition to a fine, or be only sentenced to a fine.”

616 China Judgements Online, <http://wenshu.court.gov.cn/website/wenshu/181217BMTKHNT2W0/index.html?pageId=9381f6ce018f425935c8a6e4a8022c3>

617 Guo Wei illegally possession of propagating terrorism and extremist articles. The perpetrator downloaded video of propaganda, incitement of terrorism and violence terrorism activities from the Internet and uploaded it to the Baidu cloud account and QQ group, and was finally sentenced to two years in prison in 2018. '闽05刑初字65号'(Min 05 Xing Chu Zi No.65)'(China Judgement Online, 2018)<http://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?docId=367f66fe4dd4444a6f6a992009cb6e2> accessed 20 Sep 2020.
arbitrariness in the application of convictions and penalty measures. A comparison could be drawn here with the important precursor offence in E&W regarding possession for terrorist purposes under the TA 2000, which are s 57 (possession of items) and s 58 (collection of information). However, unlike E&W, the Chinese provision (Art. 120f) does not require a reasonable suspicion that the possession be related to committing, preparing, inciting or other acts connected with terrorism.

5.6 Aggravated Punishment for Terrorism

The development of China's counter-terrorism laws is further exemplified by the penal arrangements for terrorist offences under the CL. According to Liu Renwen and Ni Chunle, China's anti-terrorism laws are characterised by emergency reaction and a tendency to take strict and stern measures. Firstly, in Amendment (III), the sentencing range for those who organise and lead a terrorist organisation was increased from 3-10 years to a mandatory minimum of 10 years. Additionally, the legal punishments for organisers, leaders and active participants were distinguished, and the statutory sentences for the former two were aggravated. This shows that Chinese criminal law has tended to use increasingly severe penalties to combat offences related to terrorist organisations.

Secondly, a “terrorism connection” is also an aggregate offence, and carries the maximum punishment of the death penalty. For example, as the maximum punishment of perpetrator committing murder, explosion, and kidnapping is the death

---

619 Details will be found in Chapter 7.
621 China’s Criminal Law, Art. 120 Para. 1: “Whoever organizes or leads a terrorist organization shall be sentenced to a fixed-term imprisonment of over 10 years or life imprisonment; those who actively participate in a terrorist organization shall be sentenced to a fixed-term imprisonment ranging from 3 to 10 years; other participates shall be sentenced to a fixed-term imprisonment of less than 3 years, criminal detention, public surveillance or deprivation of political rights.”
622 Zhou Zunyou, Balancing Security and Liberty: Counter-Terrorism Legislation in Germany and China (Dunker & Humblot 2014) 140.
623 China’s Criminal Law, Art. 120 Para. 2: “Whoever commits the crime in the preceding paragraph and also commits murder, explosion, or kidnapping shall be punished by an aggregate sentence.”
penalty in China’s CL, then the maximum aggregate sentence for ringleaders or participants of a terrorist organization my ultimately be the capital punishment.

Thirdly, Amendment (VIII) further increased penalties to curb terrorist activities, and expanded the scope of “special recidivism,” stipulating that terrorist activists are in the practice of establishing special recidivists. Such special recidivists are now subject to heavier punishment. Fighting terrorism by increasing penalties has also been one of the key elements of the punitive anti-terrorism strategy in China. According to Wang, since terrorists’ cyber activities are anonymous and likely to cause social panic, such activities should be punished severely as a means of prevention.

Fourthly, the counterterrorism legal framework still relies on a punitive strategy. If the continuously revised and promulgated law on terrorism is the first line of defence against terrorism, then the second line of defence is the application of harsh punishment and sentencing for terrorism-related offences in judicial practice in China. Some scholars have claimed that the Chinese government’s main strategy in counteracting terrorism before 2001 had been punitive. Driven by the State’s enactment of the Strike Hard campaigns to combat crime in the reform era (1980s–1990s), the Chinese government relied heavily upon punitive strategy to combat the offences that endanger national security and social stability. Repressive measures including arbitrary arrests, public sentencing, swift adjudication and harsh punishments were employed by law enforcement agencies to generate a deterrent

---

624 Applicable solely to terrorism-related crimes, organized crimes, and crimes which threaten national security, special recidivism refers to circumstances where an offender recommits an offense at any time after serving the sentence or being granted an absolution, after which the recidivist is subject to a sterner punishment than ordinary re-offenders.

625 China’s Criminal Law, Art.66. The old provision provides that criminals only endangering national security constitute special recidivists, but the new provision was expanded as “jeopardizing the national security, terrorist activities or organized crimes” are all to be treated as recidivists. Then the special recidivist shall be given a heavier punishment.


628 During the reform period, three nationwide strike-hard campaigns were initiated in 1983, 1996, and 2001, respectively, with numerous small-scale campaigns launched at the local level.

629 Punitiveness is a criminological concept of assessing punishment, which refers to connotations of excess-that is, "the pursuit of punishment over and above that which is necessary or appropriate.” Rogue Matthews, The Myth of Punitiveness,9(2) Theoretical Criminology 179 (2005).
effect and to educate the public that terrorism was intolerable in Chinese society. 630 In this section, the definition of punitiveness will be applied in the CTL, the CL and other counter-cyberterrorism-related legislation and punishments, because these pieces of legislation and their derive sanctions should be put together as the legal framework to combat cyberterrorism. 631 Through the above analysis, in the context of anti-cyberterrorism in this section, punitiveness is considered the intensification of laws and punishments, specifically to extend the duration of sentencing in law and to increase the severity of punishment in practice.

Furthermore, through an analysis of the evolution of anti-terrorism legislation, as shown in the above-mentioned aggravated punishments, China has developed a more punitive anti-terrorism legal framework in the post-2001 era. Affected by the "9.11" incident in the US, anti-terrorism legislations in most countries of the world is contingent, 632 and China is no different. For example, as many as nine provisions in Amendment (III) adopted, all of which refer to terrorist crimes, where it is clearly stated that it is ‘targeted to some new situation of the terrorist activities that have recently emerged, and in order to crack down on terrorism strictly.’ 633 It can be seen that no matter from the breadth or intensity of criminal law intervention, it shows obvious attitude of harsh punishment and strictness.

In addition, according to a work report, the SPC severely punishes crimes that endanger national security and violent terrorism:

632 A common feature of these emergency legislation is the expansion of the power of the police and intelligence services to obtain information about terrorists and terrorist activities. Although strict conditions and procedures are imposed on the exercise of these powers, legislators are still not at ease, so some countries have set up “sunset clauses”, such as the "Anti-Terrorism Law” enacted by Germany in 2001, which requires the legislature to Review once to decide whether to extend the applicable period of these laws. In addition, in many countries, such anti-terrorism laws for emergency response can also be restricted by launching a constitutional review mechanism. More details see Zhou Zunyou, ‘Development of German Anti-terrorism Legislation’ (德国反恐立法的发展) (Proceedings of the Symposium on Social Stability and Anti-Terrorism, Beijing, 13 October 2012).
We will safeguard the political security of the country, especially the security of the regime and system, and strengthen the fight against terrorism, anti-secession and anti-cult, and severely punish crimes such as inciting secession and subversion of state power in accordance with the law, and earnestly safeguard national security. In conjunction with the relevant departments, it issued opinions on violent terrorism and religious extremism criminal cases, and severely punished tyrannical crimes such as “10.28 Tiananmen Square incident” and “3·01 Kunming incident” in accordance with the law, and maintained the overall stability of the society.634

The SPC report highlighted that ‘crimes of endanger national security and violent terrorism should be punished severely…. increase penalties for inciting separatism, organizing, leading and participating in terrorist organizations, and disseminating terrorism videos.’635 According to the statistics of the SPC, there were 558 cases involving incitement to separatism, violent terrorist attacks and so on in 2014, which increased by 14.8% compared with 2013, and 712 criminals were sentenced (up by 13.3% compared with 2013).636 By 2015, the courts at all levels in the country had concluded a total of 1,084 crimes against national security and violent terrorist crimes (up by 94.3% year-on-year), and sentenced 1419 criminals (up by 99.3% year-on-year).637 This demonstrates that terrorist and extremist crimes have shown an upward trend in China in recent years. At the same time, it also reflects the country's efforts to increase punishment and expand the scope of criminalisation. To deal with any attempts to subvert state power and create ethnic contradictions, the Chinese government's policy is to fight early and not allow such activity to spread, and to prevent terrorism and extremism from gaining any momentum.

This is not only exemplified by the courts' increased imposition of the severest sanctions (e.g. the death penalty and life imprisonment) in the context of the State's

---

635 Ibid.
pursuit of “social harmony” by adopting the “Balancing Leniency and Severity (宽严相济)” policy, but is also demonstrated by the ways in which terrorist offenders are essentially tried and sentenced in the adjudicative process.638

Balancing Leniency and Severity is a new crime control strategy which was promoted by Chinese SPC and has served as basic criminal justice policy since 2005. It is premised on the idea of tempering harsh punishments for a selection of extremely serious crimes with lenient treatment for the majority of crimes which are minor or carried out with mitigating circumstances.639 One of the stated goals of this policy is to mitigate potential social instability created by the effects of the State’s propensity for harsh punishment over the last 30 years.640

With the strengthening of its anti-terrorism laws since 2001, China has justified criminalisation on strong legal grounds.641 To be fully retributive, the punishment must be proportionate to the gravity of the crime.642 Therefore, criminalisation reduces penal punitiveness by penalising terrorist offenders in a rational manner. More notably, in criminalising terrorist offenders, harsh penalties are not as indiscriminately and erratically applied as they are during crackdowns.643 Instead, the legal apparatus metes out death sentences and even lengthy imprisonment in a way that reflects the individual's degree of criminality and personal circumstances. This reflects the authorities' attempt to abide by the penal policy of “Balancing Leniency and Severity (宽严相济)”.

641 Over the past two decades, the Chinese government has revised and passed a spate of laws on Counter-espionage, National Security, National Intelligence, Counter-terrorism, Cybersecurity and Foreign NGO Management, and not to mention the two instrumental pieces of legislation - the Criminal Law and the Criminal Procedure Law. Such interconnected package of counter-terrorism, national security and law enforcement legislation repeatedly obligates citizens, organizations and companies to provide cooperation and support for police activities that tackle terrorism. See MS Tanner, ‘Beijing’s New National Intelligence Law: From Defense to Offense’ (Law Fare, 20 Jul 2017) <https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense> accessed 8 November 2020.
643 Human Rights Watch, ‘China: Disclose Details of Terrorism Convictions. Overboard Counterterrorism Legal Framework Opens Door to Abuses’ ( Human Rights Watch, 16 Mar 2017)<https://www.hrw.org/news/2017/03/16/china-disclose-details-terrorism-convictions> accessed 21 May 2020. In this report, four terrorism-related cases handled in 2016 were observed and the sentences of seven offenders varied from case to case, ranging from the exemption of criminal penalties to three years of imprisonment.
"严相济)" when sentencing serious crimes in a more nuanced manner, as it involves 'the application of, when appropriate, relatively harsher penalties in some minor cases and relatively lighter penalties in some serious cases (Yanzhongyoukuan, Kuanyijian, Kuanzhongyouyan, Yanyijikuan).'

However, the increased use of soft penalties for certain crimes does not necessarily indicate the reduced application of heavy punishments. Rather, the debate about heavy punishment has shifted to the question of whom to 'strike hard' thereby confining severe punishment to a smaller group of the "most serious criminals." Although the CL lacks an exclusive list of the most heinous crimes, harsh sanctions are reserved for those who have committed offences endangering the core interests of the State. As such, on the one hand, the Chinese government has begun to downplay harsh justice, as demonstrated by the relatively limited use of the death penalty for certain crimes (e.g. economic and white-collar crimes), as well as the abolition of two notorious coercive measures in administrative justice: custody and repatriation; and re-education through labour. On the other hand, severe sanctions have not only persisted, but have been upgraded to deal with terrorism-related crimes because of their heinous nature and threat to national security. The unified sentencing model has moved on from the rigorous justice of the 'strike hard' era, but is now driven by nationally standardised and strengthened sentencing rules to continue the fight against terrorism in the new era.

Using criminalisation rather than the 'strike hard' campaign or crackdowns reflected the CCP’s pursuit of a rule of law strategy for counter-terrorism. However, in China’s one-party state, law, particularly criminal law, has been deeply embedded in the CCP’s political ethos and has largely served as a manifestation of political will and as a lever

---

644 S Trevaskes, The Death Penalty in Contemporary China (Springer 2012)214.
of social control.\textsuperscript{649} Despite calls for the rule of law and judicial fairness in Hu’s and Xi’s administrations, law in the criminal justice system has never been able to distance itself from political influence and interference.\textsuperscript{650} Counter-terrorism laws are not an exception here. When terrorism is perceived as a tenacious impediment to state sovereignty and national security, the CCP will most likely reform the terrorism laws without restraints and without regard for norms in the State’s actions to fight terrorist threats.\textsuperscript{651} The legislative modifications are relied upon as “lawful” vehicles to carry and deliver the CCP’s paradigm shifts in counter-terrorism. This may explain the absence of due process considerations in the Chinese criminalisation process of terrorist acts. This explanation shows, particularly, that China’s due process is not devised to strike a balance between civil liberties and national security in comparison to many counter-terrorism law developments in Western jurisdictions attempt to do.\textsuperscript{652} In short, it is more precisely a process that justifies and legitimises the use of state authoritarian power to penalise acts that endanger the Party’s political stability under a cloak of legality.

5.7 Vague and Uncertain Criteria of Measuring the Severity of “Circumstances”

However, due to the ambiguous definition of terrorism and the criteria for measuring the penalty, it is likely that similar offences could draw different punishments across provinces. For example, although the central authority provides basic legal documents that guide the local authorities in practice, the vague criteria in determining the “circumstances” of the crimes allows the local authorities to interpret the law as they see appropriate.\textsuperscript{653} It gives the judiciary power and pressure to identify the severity of

\textsuperscript{649} ibid.
\textsuperscript{650} ibid.
\textsuperscript{653} For example, an offender in Hunan province was given 13 days in detention and an 8000 RMB fine for uploading terrorist videos to a Wechat group, while in a similar case, an offender in Sichuan province was given 10 days in detention, and another offender in Shanxi province was given 5 days in detention for uploading terrorist video clips. See Jiangxi Provincial Public Security Department, ‘Public Security Services Remind You: Do Not Wait until Arrest to Learn This Is Illegal’ (Jiangxi Public Security, 5 Jan 2017) <http://www.jxga.gov.cn/news/lingshiluiao/2017-01-
the “circumstances” to maintain justice.\textsuperscript{654} Judicial organs should abide by the principle of "Balancing leniency with severity" but in the context of counter-terrorism, some cases have been severely punished only for being suspected of links with terrorism,\textsuperscript{655} which reflects China's tendency to combat terrorism by applying the principle of strictness. Given this, the equality principle and due process could be violated and undermined.

However, there are no official documents providing instructions on how the punishment should be applied. Essentially, the criteria for the measurement of the severity of “circumstances” are not clear enough to prevent abuses of power. Given this vague language and the uncertain standards, one cannot predict whether their actions will violate the law, and this in turn violates the legal principle of certainty.

The vague language of terrorism-related provisions in the CTL and the CL may result in the Chinese government using legislation as a tool to over-criminalise terrorism-related offences. Some commentators believe that, similar to many other laws and regulations in China, the vague CSL was designed to give the authorities more flexibility and leeway to interpret and implement it.\textsuperscript{656} For example, the authorities in charge may apply a case-by-case approach to interpreting the law.\textsuperscript{657} Such an interpretative approach may result in selective prosecution. Indeed, regulators may harshly enforce the law against disobedient people or companies who have become a thorn in the side of the nation-state.\textsuperscript{658} Therefore, a more fundamental concern in terms of the new law is probably not the vagueness of its language but, rather, the fact that the country has few democratic checks and balances.\textsuperscript{659} In view of this, many grey areas are generated when the law is enforced. Due to the ambiguity of counterterrorism legislation above-mentioned, how to enforce these laws and what their real impacts are depend on regulators’ interpretation. Therefore, the Chinese

\textsuperscript{655} Zhang Chi, ibid.
\textsuperscript{657} E lasiello, ‘China’s Cyber Initiatives Counter International Pressure’ (2017)10(1) JSS 1, 8.
\textsuperscript{658} ibid.
\textsuperscript{659} ibid.
government needs to consider all aspects of the circumstances during the implementation of these laws.

Due to the vagueness and extensiveness of the wording of the legal provisions, arbitrary interpretation and expansion of punishment may materialise in judicial practice. For instance, there is no uniform applicable standard across the country, and different local courts give different judgments for similar cases, ranging from 15 days detention to lifetime imprisonment. In the case of Wang Bingzhang, he was accused of uploading and publishing a number of terrorism propaganda articles, and organising and leading violent terrorist activities. Eventually, he was sentenced to lifetime imprisonment. However, in the case of Wang, he was accused of downloading numerous videos of ISIS's violent terrorism activities out of curiosity, and was finally sentenced to 15 days of detention. This shows that in judicial practice, different local courts interpret the seriousness of the circumstances differently, so there is a huge gap in the judgment results across provinces, which violates the principles of certainty and commensurability.

5.8 Broad Discretion of Executive Organs to Designate Proscribed Terrorist Organisations

Initially, the designation power was completely in the hands of the executive (National Counter-terrorism Leading Organ), but then the CTL 2015 empowered the judiciary to designate terrorist organisations and individuals. Therefore, the “double track system” of terrorist designation means both the executive and judiciary are in charge.

---

of the designation of terrorist organisations and individuals. However, the reliance in practice is heavier on the executive. According to Chapter II of the CTL 2015, the National Counter-terrorism Leading Organ (NCTLO) has the power to designate terrorist organisations and individuals. The procedure of designation involves all levels of executive power and then the list is signed by the Premier of State Council and published as an official gazette. The broad definition of terrorism may result in a degree of flexibility and arbitrariness for executive agencies in the designation of terrorist organisations and terrorists.

Many Chinese scholars are optimistic about the effectiveness of the double-track system and believe that it has greatly reduced the burden on the prosecutor during the prosecution process. Some scholars have argue that the double-track system can effectively prevent terrorism because it can help the Chinese government to actively identify potential terrorist threats before actual crimes occur. According to Jia and Li, executive designation is a pre-emptive strategy and is a supplementary measure of judicial designation based on facts and evidence. However, Xia and Lan et al. have critically highlighted that the boundary between executive designation and judicial designation is not clear. Zhang Lei proposed that these two forms of designation

---

664 The details of “double track system” of terrorist designation could be found in Zhang Chi (n 25) 161.
665 Article 12 of the Counter-Terrorism Law stipulates that the working body of the National Counter-terrorism Work Leading Organ shall designate terrorist individuals or groups, while Article 16 stipulates that the intermediate, or above people’s court, shall determine terrorist organisations and individuals pursuant to the Criminal Procedure Law. Zhang Chi, ibid 160.
666 To propose a designation, the departments of public security, and state security, the Ministry of Foreign Affairs and the provincial Counter-terrorism Leading Organ files an application to the National Counter-terrorism Leading Organ. Public security departments and security departments (executive) at all levels oversee, investigate, and gather evidence about the suspected entity, and escalate this to higher levels all the way to the Minister of Public Security who then reports directly to the Premier.
are complementary, but with the main reliance being placed on judicial designation and executive designation being supplementary.\textsuperscript{672}

Because of the wide-ranging executive power of terrorism designation, some problems with due process have arisen. Firstly, the executive designation of terrorism contravenes the presumption of innocence as stipulated in the Criminal Procedure Law (CPL, Art. 12).\textsuperscript{673} Xu Shanghao argued that the evidence collected by the NCTLO is admissible in court.\textsuperscript{674} Secondly, the CTL does not explicitly stipulate the procedures through which the executive should accept and publish the judgments made by people’s courts. So far, in addition to the three official lists,\textsuperscript{675} the NCTLO has not yet published a list of designated individuals and organisations as previously released by the judiciary.

Thirdly, no independent review or supervision is carried out by other departments about the designation mechanism.\textsuperscript{676} The designation body itself is also the review body, the result of which is to make a decision to uphold or revoke a designation.\textsuperscript{677} Some Chinese scholars have expressed doubts about the establishment of an external review procedure. Sun held that allowing judicial and societal oversight of the review process would undermine the authority of the NCTLO (the highest counter-terrorism executive body).\textsuperscript{678} Xu considered that judicial supervision should be established because justice is the last line of defence to prevent abuses of power.\textsuperscript{679} In addition,


\textsuperscript{674} He invoked Section 52.2 of the Rules for Criminal Procedure of the People's Procuratorate which gives the executive the power to collect legal evidence. Xu Shanghao, ‘Research on the Designation Process of Terrorism Organisations and Individuals (恐怖活动组织与人员的认定程序研究)’ (2016) 3 Shandong Social Sciences 115.

\textsuperscript{675} The National Counter-terrorism Leading Organ has issued three lists of terrorist organisations and individuals which include 4 organisations and 25 individuals. The designation of some entities and individuals, such as the World Uyghur Congress and Dolkun Isa, is highly controversial. Zhang Chi(n25) 149.

\textsuperscript{676} Article 15 of the Counter-Terrorism Law stipulates that designated individuals and organizations can appeal to the National Counter-terrorism Leading Organ – the designation body itself. Zhang Chi (n25) 162.


\textsuperscript{678} Xu Shanghao, ‘Research on the Designation Process of Terrorism Organisations and Individuals (恐怖活动组织与人员的认定程序研究)’ (2016) 3 Shandong Social Sciences 112–118.
Guo proposed a compromise, namely internal supervision, which means the review process should be carried out by different departments within the NCTLO. However, discussion about the establishment of independent review and supervision has only occurred at academic level so far. In the absence of an independent review body, so far no official information has been published for review or delisting procedures, and no cases of appeal have been heard in practice. Dissidents and rights organisations have questioned the legitimacy of China’s terrorism designation, raising the issue of abuses of power by the executive. For example, Amnesty International conveyed its concerns over the dangers of calling a peaceful political opposition group a “terrorist organization.”

Fourthly, according to the above-mentioned Zhao Yongchen, the official criteria for terrorist designation should be satisfied both the membership of terrorist organisations and carrying out terrorist activities. Accordingly, China’s official designation of terrorist individuals is not based merely on their association with designated organisations. However, in practice, this standard does not seem to be strictly followed. For instance, in the controversial case of Ilham Tohti, a former professor at Chinese Minzu University was classified as a terrorist. However, in the eyes of many in the West, he is a "human rights fighter" and won the US Human Rights Award for his efforts in “Anti-Oppression.” It thus appears that China’s terrorism designation mechanism may violate citizens’ freedom of association.

---


682 He said the designation of individuals must satisfy the following two criteria at the same time: (1) Association with terrorist groups, and engagement in activities that endanger national security and the life and property of individuals. (2) Engagement in any of the terrorist activities. Zhang Chi (n 25) 158-159.

683 He was accused of associating with foreign separatist organisations and individuals and other offences such as spreading separatist ideology and inciting ethnic hatred. It is not clear what proportion of his association with designated groups and individuals accounts for his life sentence. Xinhua, ‘Ilham Tohti Was Sentenced to Life Imprisonment for Secession of First Intrance (伊力哈木·土赫提涉分裂国家罪一审被判无期徒刑)’ (Xinhua, 23 September 2014) <http://www.chinanews.com/gn/2014/09-23/6621587.shtml> accessed 24 Sep 2020; Zhang Chi (n 25) 163.

5.9 Enforcement of the Criminal Law and Counter Terrorism Law

From the practical perspective, the enforcement of anti-terrorism legislation in China has had an increasing focus on prevention rather than retribution. Correspondingly the vast majority of anti-terrorism laws gradually extend executive powers to interrogate, detain and control suspected terrorists during the pre-trial period. The specific characteristics of the implementation of China's anti-terrorism laws are analysed in the following sub-sections.

5.9.1 The Expanding Power of Administrative Departments (mainly the police) during Counterterrorism Efforts (such as investigation and detention)

In order to prevent terrorism, China has granted executive organs wide discretion to detain, interrogate and control suspected terrorists by amending the Criminal Procedure Law (CPL) and enacting the Counter Terrorism Law (CTL) to enable the continuous expansion of the powers of administrative agencies. These powers are often exercised without due process, in that the procedural rights of suspects that should be otherwise guaranteed are in fact constrained to the point that there is an imbalance between security and liberty in Chinese counterterrorism laws. 685 Furthermore, some Chinese scholars have proposed endowing police and prosecutors with special anti-terrorism powers (such as surveillance and investigation without a warrant), which would mean a further expansion of state powers in the name of counter-terrorism to maximise social stability and security. 686

The CPL was amended in 2012 by the NPC, which revised seven provisions related to terrorism offences, and expanded police powers to investigate terrorist offenders prior to trial, to include “technical investigation” often referred to as “secret investigation.” Technical investigation includes measures such as electronic monitoring, phone surveillance, mobile positioning, email examination, secret photography, undercover investigation and other secret approaches undertaken without suspects’ permission and awareness.

Although the legality of technical investigation has been questioned because of the ambiguity of its applicability, according to the CPL, material collected through technical investigation measures is considered valid as incriminating evidence against suspects in court. This wording differs from previous stipulations, which provided that materials derived from technical investigatory instruments can be used only to aid police investigation, but not as evidence in criminalize prosecutions.

Another controversial element of arbitrariness is the clause giving police discretionary detention powers, which permits detention of suspects involved in terrorist crimes incommunicado and in secret locations. Moreover, secret detention allows police to confine individuals suspected of terrorist offences at a designated place without issuing a notice of detention to the family if doing so could impede the investigation. This section allows for “secret detention” of suspects, raising doubts about legality and compatibility with the rule of law.

---

687 Article 148 of the Criminal Procedure Law firstly allows the use of “technical investigation” by police in terrorism cases: After the public security organ has filed a case, it may, insofar as required for investigation and after passing strict approval, take measures of technical investigation for cases involving crimes endangering state security, crimes of terrorism, organized crimes with characters of the underworld, major drug-related crimes, or other crimes that pose a serious threat to society.

688 There has been debate over what constitutes technical investigation in the Chinese criminal justice system. For a detailed discussion, see Lan Yuejun, ‘The Measures of Technical Investigation from a Comparative Perspective' (2013) 1 Journal of China’s Criminal Law 66, 66-67.

689 China’s National Security Law, Art. 10; China’s People’s Police Law, Art. 16.

690 China’s Criminal Procedure Law, Art. 150.


692 Art. 83 of the Criminal Procedure Law provides: After being taken into custody...the family members of the detained person should be informed within 24 hours, except for situations in which it is impossible to issue a notice or the detained person is suspected of committing crimes endangering state security or crimes of terrorism and family notification may impede the investigation.

693 China’s Criminal Procedure Law, Art.73.

waiving of notification of pre-trial detention in cases "involving state secrets" or when "notification would interfere with the investigation," the wording of the relevant clause is vague, leaving considerable space for authorities' overuse of their detention power. There is a lack of an explicit definition of "impediment of investigation" in law and judicial interpretations could thus result in the virtual disappearance of criminal suspects. In the 2012 revision, the detention powers are further extended to another form of incarceration instrument, namely residential surveillance (essentially, house arrest). Under the circumstance of residential surveillance, the police may implement electronic surveillance, irregular inspections and other means of surveillance during the investigation, and law enforcement agencies can monitor the communication of suspects.

5.9.2 Limited Safeguarding of Suspects' Rights in Terrorism-related Cases

With the expansion of police powers, terrorism suspects lack sufficient legal rights to ensure fair treatment in the criminal justice process. In particular, suspects have limited access to legal counsel during the investigation phase. According to Art. 37, a suspect's request to meet with their defence lawyer in cases involving national security, serious bribery and terrorism ought to be approved by the investigative organs. Hence, suspects involved in terrorism cases are more restricted in accessing of counseling of lawyers during the investigation phase. One of the other major difficulties “frequently encountered by Chinese lawyers when representing their clients,” is the police obstruction of lawyers attempting to visit their client when in detention. Not surprisingly, some scholars have questioned the extent to which the police misuse this power to minimise contact between lawyers and suspects.

---

695 According to Article 73 of CPL, the police are granted the discretion to place a suspect under residential surveillance at a designated location other than his/her domicile if residential surveillance at the suspect's domicile may impede the investigation of cases connected with terrorism.

696 China’s Counter-Terrorism Law, Art.76.

697 Article 33 of the Criminal Procedure Law states that "a suspect has the right to entrust a defense lawyer when being interrogated for the first time or placed under any custodial measures by investigative organs."


5.9.3 Empower Executive Organs with Broad Discretion to Issue Control Orders

Compared to the CPL, the newest promulgation of the CTL goes further by expanding police powers in many ways. Unlike the CPL which grants the police the ex post powers to investigate terrorist acts that have already occurred, the CTL focuses on the authorisation of pre-emptive discretion to allow the police to be proactive in its handling of terrorism. More specifically, the CTL empowers the police to take immediate lethal action when faced with violent incidents, and to impose preventive detention and control orders on suspects who are considered a great risk to national security and social stability.

Prevention under the CTL ushers in a host of "pre-crime" measures that permit the State to intervene and restrain an individual on the basis of anticipated further harm, rather than in the wake of wrongdoing. Similar to the approaches adopted in the British and Australian counter-terrorism regimes, control orders impose restraints on individuals' freedom that are not legally challengeable under the CTL or the CPL. Restraining freedom is a characteristic of many counterterrorism operations in E&W, most notably in the form of preventive detention and control orders. These measures deviate from the traditional retrospective and post-crime orientation of criminal justice systems. Against this background, a State prosecutes and punishes criminal acts based on evidence collected on past events.

However, in substance, China’s restrictive measures share many similarities with the preventive detention and control orders used in the counter-terrorism framework in E&W. Despite targeting different types of terrorist threats, the pre-crime tools used

---

701 Ibid.
703 Neither the CTL nor the CPL has established the checks and balances process for affected individuals to seek recourse.
in E&W may be preventive in nature.\textsuperscript{706} The aim of such pre-crime tools is to place restraints, prohibitions and obligations on individuals to protect members of the public from the risk of a terrorist act.\textsuperscript{707} In contrast, the restrictive measures in China are used to facilitate law enforcement activity by depriving the suspects of their individual freedoms.

Similar to E&W, China empowers the police to use control orders in the course of investigating suspected terrorist activities in the CTL.\textsuperscript{708} This new control model reflects China's constant reliance on draconian justice to manage and control the risks posed to the country and its security. In the implementation of the control orders, there may be result to harshness and arbitrariness. Most importantly, only the police (the head of public security organs) in China have the power to issue control orders, without the supervision of procuratorates and courts. This reveals a clear contrast with the control order scheme in E&W, where the prosecutor must seek a written control order from the court.\textsuperscript{709}

On the contrary, the standard for issuing control orders in China lacks clarity and transparency. Akin to many custodial measures in China's criminal justice system, the enforcement of control orders is not a neutral judicial decision, but the result of the police's exercise of its powers of detention. This enforcement reflects China's legal tradition whereby the police are the only interpreters of vague legal provisions relating to incarceration. Therefore, the controversies that may arise from these control order clauses reflect the unfairness of their application when the police act arbitrarily without considering scientific evidence and supervision of courts and procuratorates.

\textsuperscript{706} C Walker, 'The Reshaping of Control Orders in the United Kingdom: Time for A Fairer Go, Australia' (2013) 37 UMLR 143, 150.


\textsuperscript{708} In light of Article 53, suspected terrorists, upon the approval of the head of public security organs above the county level, should be subject to one or several restrictive measures depending upon the level of their dangerousness. More precisely, those suspected of terrorist acts are: (i) not allowed to leave the residential city, county, or the designated residence without the approval of the police; (2) not allowed to participate in large public functions or special events; (3) not allowed to take public transportation or enter into special venues without the approval of the police; (4) not allowed to meet or communicate with certain designated persons; (5) required to report to the police on daily activities on a routine basis; (6) required to hand in passport, identification card, and drivers' license for the police to keep.

Furthermore, the police’s issuance of control orders in China cannot be either internally or externally challenged. In the control order system of E&W, even though procedural justice in control order hearings has been questioned,\textsuperscript{710} certain protections are afforded to suspects to ensure a fair outcome. For example, a person subject to a control order can apply for its revocation or variation when it is renewed, by outlining the reasons in writing to the court in E&W.\textsuperscript{711}

However, when the Chinese police are considering control orders, such procedural safeguards do not seem to exist. The legislator completely ignores the right of the controlled person to obtain legal counsel, and there is no checks-and-balances mechanism in the law that could supervise the control order. Neither the CTL nor the CPL provides for a remedy system for an independent and impartial review of the legality of the order issued by the police. Ultimately, there is no doubt that the absence of a specific human rights law in China’s legal system increases the risk of both controlees’ abuses of power and miscarriages of justice.

5.9.4 Tendency of Using Non-criminal Disruption Methods to Deal with Precursor Terrorism-related Offences

In addition to attaching criminal liability to preparatory offences, the administrative detention system functions as the second tier of control, targeting a lesser degree of similar acts which are deemed to be administrative perpetrations as opposed to actual criminal offences.\textsuperscript{712} Characterised as an adjunct to criminal punishment, administrative detention is governed by an array of administrative regulations in parallel with the criminal justice system and positioned within the framework of police powers.\textsuperscript{713}

\textsuperscript{710} S Donkin, Preventing Terrorism and Controlling Risk: A Comparative Analysis of Control Orders in the UK and Australia (Springer Science & Business Media 2013)35.
\textsuperscript{711} ibid.
\textsuperscript{713} ibid.
In the CTL, Art. 80 states that the police may incarcerate participants of the following activities for 10-15 days if the offence does not constitute a crime under the Public Order Detention. These administrative contraventions overlap to a great extent with some preparatory offences also outlined by the CL albeit with minor variations in wording. However, the boundary distinguishing crimes deserving of administrative detention and those subject to criminal penalisation is left undefined in both the CL and the CTL. Within the CTL, Art. 81 affords the police the power to jail those who are engaged in offences that make use of extremism (for 5-10 days) if the offence is not serious enough to amount to a crime and only has minor consequences.

Although criminal punishment of preparatory offences concerning terrorism is available, China seems to lean towards administrative custody more commonly when addressing potential terrorist/extremist risks. The data collected from the Case Information Disclosure System of the People's Procuratorates and China Judgment Online indicate that only a handful of individuals charged with preparatory offences were processed in the criminal justice system between August 2017 and September 2018. This contrasts quite sharply with the more than 200 individuals who were successfully prosecuted for planning, supporting or inciting terrorism in the UK between 2001 and 2008. Notwithstanding China's long-standing history of not recording administrative

714 China's Counter-Terrorism Law, Art.80: "(1) Advocating terrorism or extremism, or inciting the commission of terrorist or extremist acts; (2) manufacturing, disseminating, or unlawfully possessing items that advocate terrorism or extremism; (3) Compelling others to wear or bear clothes or symbols that advocate terrorism or extremism in a public place; (4) Supplying support, aid, or facilitation to the advocacy of terrorism or extremism or the commission of terrorist or extremist activities, such as by providing information, financing, supplies, technologies, or venues."

715 China's Counter-Terrorism Law, Art.80, Art.81.


717 By searching keywords "terrorism" in the Case Information Disclosure System of the Chinese Procuratorates, the results indicated that there were eight cases prosecuted by the procuratorates nationwide. However, no records on the relevant trials were shown by searching "terrorism" in China Judgment Online. It is perhaps due to the fact that China has treated information on terrorism-related offences as the "state secret." See Human Rights Watch, 'China: Disclose Details of Terrorism Convictions, Overboard Counterterrorism Legal Framework Opens Door to Abuses' (Human Rights Watch, 16 Mar 2017) <https://www.hrw.org/news/2017/03/16/china-disclose-details-terrorism-convictions> accessed 21 May 2020. The website for the Case Information Disclosure System of the Chinese Procuratorates <http://www.ajxxgk.jcy.gov.cn/html/index.html.> For the website for China Judgement Online, see China Judgement Online< http://wenshu.court.gov.cn/index > accessed 9 March 2019. It is noted that by searching keywords "terrorism and extremism" in one of the privately-funded case law databases, see JUFA ANL< https://www.jufaani.com/>. The results indicate that there were ten cases involving the violation of Art. 120 (2)-(6) of the CL prosecuted and tried between 2016 and 2018; Zhang Chi (n 25).

offences in its official legal database, a review of information on media reports and the police’s public WeChat platform illustrates the predominant use of the Public Order Detention to sanction individuals engaged in minor acts associated with terrorism and extremism.719 In April 2016, the first case of a violation of Art. 80 of the CTL was reported in Ji’nan, Shandong Province.720 This case marks the beginning of a host of cases in which the Chinese police applied administrative detention; for example, the local authorities of Kunming filed 224 administrative cases in relation to the CTL, in which 23 individuals were detained.721 A wide range of acts triggered this spike in police detentions but most of the offences related to watching and distributing "extremist" videos on social media.722

The tendency of using administrative detention to tackle preparatory terrorism offences has become more prominent amid China’s calls for the prevention of terrorism. The Chinese authorities have long employed administrative detention as an efficient and cost-effective approach to policing low-level offences.723 In addition, the power of administrative detention is concentrated in the hands of the police and has great practical flexibility. Therefore, it is more popular as a crime control tool in contemporary China, but it may lead to abuses of power.

However, the ambit and application of administrative detention, much like restrictive measures, is not scrutinised by a judicial review process, nor is it open to procedural

719 The results of typing keywords "administrative detention" and "terrorism" in China’s primary search engine "Baidu" show a long list of cases involving the imposition of public order detention on individuals engaged in acts which breach Art. 80 of the CTL. WeChat is a messaging and social media application widely used in China, equivalent to Facebook, Twitter or Instagram Ministry of Public Security opened its official WeChat platform in 2013 to release first-hand information on policing, criminal cases and social management.

720 In this case, Mr. Wang XX (the name is intentionally concealed by the police) was arrested for visiting foreign websites that contained violent videos of ISIS engaging in fights and committing beheadings. Mr. Wang received a fifteen-day public order detention on the basis of illegally possessing items related to terrorism and extremism. See Yang Jiaojiao, ‘The First Case Concerning the Counter-Terrorism Law in Jinan(济南涉反恐法第一条)’ (Legal Daily, 26 Apr 2016) <http://www.legaldaily.com.cn/index/content/2016-04/26/content_6602490.htm?node=20908.> accessed 13 May 2020.


checks and balances, except for the right of the detained to apply to the same decision-maker for reconsideration.\textsuperscript{724} This more or less unconstrained and unsupervised discretion may result in arbitrary restrictions of individual freedoms. From the preemptive point of view, the elastic utility of administrative detention is consistent with the prevention of the occurrence of substantial terrorist acts. More markedly, administrative detention extends the reach of the CL to penalise similar acts with a lower level of harm and severity by expanding police powers.

\subsection*{5.10 Conclusion}

In China's political context, which prioritises national security and social stability, legislators have broadened the scope of the counter-terrorism legal framework. This reflects the legal reality of "rule by law" in China, through which the CCP expands state power by broadening counter-terrorism legislation to achieve its political goals. However, the broad and open-ended nature of the anti-terrorism legislation may contravene the basic principles of certainty, proportionality, legality and minimal criminalisation. Additionally, China's counter-terrorism approach is constrained by authoritarian characteristics such as a lack of checks and balances for human rights protection, a lack of independent judicial review for executive powers, the prioritising of national and collective interests over individual interests, and the prioritising of substantive justice over procedural justice in the context of counter-cyberterrorism legal practice\textsuperscript{725}.

Through a critical evaluation of the existing anti-terrorism legislation which could be applied to cyberterrorism, this chapter has highlighted some convergent tendencies in the legal responses of China and E&W to cyberterrorism. These similarities could be categorised into: substantive counter-terrorism laws (prevention tendency, broad and vague definition of terrorism, over-criminalisation, broad discretion of executive for designation); enforcement of counter-terrorism laws (expansion of executive powers,

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{724} E Li, 'Fighting the Three Evils: A Structural Analysis of Counter-Terrorism Legal Architecture in China' (2019) 33(3)EILR 311, 357.
\item \textsuperscript{725} Gao Juan, 'Procedural Justice over Substantive Justice: A Inevitable Choice for China's Contemporary Path towards the Rule of Law(现代中国走向法治的必 然选择——程序正义优先于实体正 义)' (2007) 2 Legal System and Society 740–41.
\end{itemize}
\end{footnotesize}
limited safeguards for suspects' rights, tendency of applying non-criminal disruption methods); and punishment of terrorist offences (aggravated punishment for terrorism).
Chapter 6 Legal System in England & Wales (E&W)

6.1 Introduction

This thesis attempts to compare the legal responses to cyberterrorism of China and E&W, and then explore whether the relationship between the respective legal systems and legal responses is necessary or contingent in countering cyberterrorism. Essentially, the question is whether a country’s legal and constitutional order has an impact on the way it responds to cyberterrorism in the absence of legislation. I seek to determine whether the divergence in constitutional order between China and E&W has also resulted in a divergence in the impact of their non-specific legislative responses to cyberterrorism. To arrive at an answer, it is necessary to review issues such as the rule of law, legal principles and the broader context of E&W's legal system.

This chapter aims to provide an overview of the legal system and the application of the rule of law in E&W, which should serve as the foundation for establishing whether the distinctive legal system of E&W matters in explaining its legal responses to cyberterrorism.

Firstly, this chapter starts by outlining the distinctive characteristics of the legal system of E&W, which includes the rule of law, supremacy of law, separation of powers and judicial independence. These principles run through the jurisdiction’s terrorism-related legislation as well. In light of this, its anti-terrorism approaches are subject to a certain degree of judicial review, independent review, legislative scrutiny and ought to take into account the safeguarding of suspects’ rights.

Secondly, another task of this chapter is to explain the basic criminal law principles which could be applied to assess the existing legal response to cyberterrorism. E&W's legal response, via criminal law, is underpinned by a particular conception of the rule of law, emphasising principles of legality, proportionality, maximum certainty, non-retroactivity, minimalism and harm. To buttress this, E&W's courts can judicially review executive decisions/actions to ensure compliance with the rule of law.

6.2 Constitution in E&W
The term “constitution” has both broad and narrow meanings. According to the narrow meaning, a constitution means a document possessing special legal status which sets out the framework and principal functions of the organs of a government within a state and declares how those organs must operate. In countries following this narrow interpretation, the written constitution has a special sanctity and is supreme over other ordinary laws, while, generally, a supreme court is established to applying the constitution to adjudicated issues. China’s constitution falls under the narrow category. However, unlike China, there is no codified constitution in E&W, as its constitution is rather a series of scattered written sources including statutes, judge-made case law and international treaties. This means that the rule of law, parliamentary sovereignty and court decisions fundamentally define E&W’s "unwritten constitution." Jeffrey Jowell acknowledged that although the unwritten constitution of E&W may have certain advantages, such as flexibility, it is accompanied by disadvantages of incoherence and inaccessibility, such as the increasing discretion of ministers and other public officials ‘untroubled by any judicial oversight or review.'

Therefore, E&W’s constitution is of the wide type. In the modern context, the House of Lords Committee on the Constitution provided a helpful definition:

that set of laws, rules and practices that create the basic institutions of the state, and its component and related parts, and stipulate the powers of those institutions and the relationship between different institutions and between those institutions and individual.

Constitutional law is pervasive across a variety of legal disciplines. Counter-terrorism is no exception, especially since the government is responsible for protecting its people and may seek extraordinary powers to perform this duty. In the context

727 The 1982 Constitution Code of the PRC.
of legal responses to cyberterrorism, constitutional law not only regulates the division of powers and interaction between different organs of the State, but also regulates the relationship between the individual (the public at large, as well as the specific terrorist suspects) and the State, protecting fundamental human rights during the implementation of counter-terrorism measures. In order to be deemed “constitutional,” executive action must be in accordance with established constitutional doctrines, and relations between the individual and the State should be “founded on and governed by law.” These above-mentioned concepts are covered by the “rule of law” doctrine. The British Constitution consists of three basic principles: the separation of powers; the supremacy of Parliament; and the rule of law. The existence of such constitutional principles does not eliminate friction between the executive and the judiciary, but prevents the rise of arbitrary executive power.

6.3 Rule of Law in E&W

The rule of law is central to the British constitution, and so we would expect legislative responses to terrorism to reflect such values. However, there is no concrete definition of the rule of law, and so in this section we set out a conception of the rule of law for the purposes of this thesis.

The rule of law is the foundation of the British Constitution and runs through the various fields of legislation in E&W. However, anti-terrorism legislation implemented after 9/11 has been widely criticised for apparently violating the rule of law. Thus, it is necessary to explore the definition of the rule of law even if doing so ‘is an exceedingly elusive notion’ resulting in a ‘considerable diversity of opinions as to its meaning.’

737 ‘The Rule of Law as a Concept in Constitutional Discourse’ (1997) 97 (1)CLR 1, 1.
with the doctrine falling prey to abuse." Dicey’s explanation of the rule of law was composed of three central tenets: ‘the absolute supremacy of regular law as opposed to prerogative or arbitrary power...second, equality before the law...third, that constitutions are not the source but the consequence of individual rights defined and enforced by courts.”

Although the UK Constitutional Reform Act 2005 (CRA) identifies and endorses the rule of law, it does not define it. The CRA explicitly recognised the persistence of an independent judiciary and the rule of law. It seems that the Parliament deliberately leaves the task of definition to the judiciary. Tom Bingham suggested that ‘the authors of the CRA 2005 recognized the extreme difficulty of formulating a succinct and accurate definition suitable for inclusion in a statute, and preferred to leave the task of definition to the courts if and when occasion arose.’

Although the rule of law is a nebulous concept, for the purpose of this thesis the following definition is adopted. This thesis argues that the rule of law includes some important criteria such as supremacy of law, adequate safeguarding of fundamental human rights protection, ensuring due process and limited arbitrary power, all of which could be applied to evaluating the existing anti-cyberterrorism legislation in E&W.

(1) The first criterion of the rule of law is that the law is freely accessible and, so far as possible, intelligible, clear and predictable. Lon Fuller argued that the coherence of the law as a system is valuable in itself – something he called the “internal morality” of law, which requires that the law must be uniform, knowable and followable. So,

---

742 S.1 of Constitutional Reform Act 2005 states that the Act does not adversely affect “the existing constitutional principle of the rule of law”.
743 Lord Bingham introduces the detail of the rule of law through his consideration of 8 implications, or sub-rules, T Bingham, *The Rule of Law* (Penguin 2011) 5.
according to the rule of law, citizens should be able to clearly ascertain and be guided by law in order to understand what is expected from them so as to avoid criminal liability.746

However, through a review of existing anti-terrorism legislation, presented in the next chapter, it seems to have deviated from this standard. Some find it particularly troubling that offences and definition are drafted in broad and unclear terms. According to the Report of the Eminent Jurists Panel on Terrorism, Counter-terrorism and Human Rights, dangers are inherent in vague or overbroad legislation.747 Furthermore, vague and overbroad terrorism-related offences may extend to the capture of a wide range of acts. Therefore, this criterion requires that all counter-terrorism measures be certain and precise to the maximum extent.

(2) The second criterion of the rule of law is that ‘the law must afford adequate protection of fundamental human rights.’748 This was supported by Lord Neuberger, who held that ‘the law must be enforceable unless a right to due process in criminal proceedings, a right to protection against abuses or excesses of the state…’749 Hart argued that people must be given ‘a fair opportunity’ to exercise the capacity for ‘doing what the law requires and abstaining from what it forbids.’750 So, in the context of countering cyberterrorism, the law must ensure due process and protect the individual’s rights from arbitrariness.

(3) The third criterion of the rule of law is that ‘the authorities at all levels must exercise the powers conferred on them reasonably, in good faith, for the purpose for which the

750 HLA Hart, Punishment and responsibility: Essays in the philosophy of law (Oxford University Press 2008)152.
powers were conferred and without exceeding the limits of such powers.\(^{751}\) Jeffrey Jowell identified the rule of law limits the abuse of power, requires that power be fairly exercised, and is enforced through judicial review.\(^{752}\) Meanwhile, Dicey associated the rule of law with rights-based liberalism and judicial review of governmental action.\(^{753}\) Thus, Dicey’s conception of the doctrine incorporated an understanding that it was the courts rather than a constitution which checked the legality of an act.\(^{754}\) Therefore, the state’s power in counterterrorism must be governed by a rule of inverse proportion: the broader the state’s power the more strictly the state must be restrained by law.\(^{755}\)

Friedrich von Hayek followed Dicey and believed that the core element of the rule of law is that no arbitrary power is in the hands of the state. He stated that government in all its actions is bound by rules fixed and announced beforehand; rules which make it possible to foresee with fair certainty how the authority will use its coercive powers in given circumstances, and to plan one’s own individual affairs on the basis of that knowledge.\(^{756}\) Thompson clearly agreed with von Hayek’s view that the rule of law is a necessary means of limiting potential abuses of power.\(^{757}\) Joseph Raz shared a common position with Thompson, von Hayek and Dicey about minimising the dangers of exercising discretionary power in an arbitrary way.\(^{758}\) With this in mind, the goal of the rule of law is to protect people from the arbitrariness of the "rule of man" and abuses of power by the state that violate individual freedom.

(4) The fourth criterion of the rule of law is the supremacy of law, which means that both state and citizens are bound by law.\(^{759}\) In this regard, Dicey also argued: ‘equality before the law.’\(^{760}\) Therefore, the executive does not have untrammelled power to lock people up.\(^{761}\) The judicial case of \textit{M v Home Office} is a good example to prove that

\(^{751}\) T Bingham, \textit{The Rule of Law} (Penguin UK 2011) 5.
\(^{756}\) FV Hayek, \textit{The Road to serfdom}, (University of Chicago Press 1994).
\(^{759}\) T Bingham, \textit{The Rule of Law} (Penguin UK 2011) 5.
\(^{760}\) In \textit{Liversidge v Anderson}, the core of the dissenting judgement was that the executive
government ministers are not above the law.\textsuperscript{762} E&W’s legal system ensures that the rule of law principles are upheld through judicial review.\textsuperscript{763} Dicey argued that the courts represented the vanguard of individual rights, and that these rights were guaranteed best by judicial decisions rather than written declarations.\textsuperscript{764}

Discretion is prevalent in E&W’s legal system. Therefore, the modern interpretation of Dicey’s first principle may be better considered as a necessary condition for proper checks of government power, and for legal authorisation to be required for the use of such powers.\textsuperscript{765} For example, overbroad terrorism precursor offences may capture both wrongful and innocent conduct, giving wide discretion to police and prosecutors to determine against whom the offences should be enforced. As these broad discretionary powers may lead to the risk of abuse of power, Edwards argued that these offences are objectionable due to their capacity to ‘oust’ the jurisdiction of the court.\textsuperscript{766}

All four of the above criteria reveal the mechanics of the rule of law and how this could be applied to examine the existing anti-terrorism legislation dealing with cyberterrorism issues. All in all, the rule of law standards could be summarised as follows: maximum certainty of definition; non-retrospective; certain and accessible; independent judiciary; fair hearings; and no arbitrary discretion.\textsuperscript{767} The rule of law standards represent the basis to protect individual autonomy, freedom and human rights, and are important

had to rule in accordance with the law. Even in times of war, the courts could not simply accept without question the executive’s view of what was reasonable. So, the executive couldn’t lock up a person without evidence because they thought it was necessary, they had to at least be able to justify this in a court to be in accordance with the law.

\textsuperscript{762} M v Home Office [1992] 2 WLR 73, 80.

\textsuperscript{763} R (Corner House Research) v Director of the Serious Fraud Office [2008] UKHL 60; see further J Jowek, ‘The Rule of Law today’ in J Jowel and D Oliver (eds), The Changing Constitution (4th edn, OUP 2000) 15-18: ‘The day to day, practical implementation and enforcement of the Rule of Law is through the judicial review of the actions and decision of all officials performing public functions’.

\textsuperscript{764} [the rule of law means] that with us the law of the constitution ... are not the source but the consequence of the rights of individuals, as defined and enforced by the courts; that, in short, the principles of private law have with us been by the action of the courts and Parliament so extended as to determine the position of the Crown and of its servants; thus the constitution is the result of the ordinary law of the land.


\textsuperscript{765} TRS Allan, Constitutional Justice: A Liberal Theory of the Rule of Law (OUP 2003) 31.


factors to consider when evaluating criminal offences, especially in the context of countering cyberterrorism.  

6.4 Separation of Powers

This doctrine refers to the separation of the three arms of the state: legislature, executive and judiciary. Montesquieu held the view that in order to resist abuses of power by a government and to ensure the protection of individual freedom, it was necessary to separate legislative, executive and judicial powers. The theoretical basis for this was that all such powers cannot be held in the hands of one person or a group, because this would lead to a lack of checks and balances and supervision, thereby giving that person or group absolute control.

Bradley and Ewing argued that the separation of powers is actually a checks and balances mechanism that allows each branch to control another branch and prevents a feature from usurping excessive power. Therefore, the overlaps, control and checks and balances of each branch need to be further analysed because they provide oversight and scrutiny of executive measures with respect to terrorists’ detention, control and designation, among other aspects. Pertinently, Lord Justice Sedley stated: ‘when the idea of rule of law is interpreted as a principle of constitutionalism, it assumes a division of governmental powers or functions inhibits the exercise of arbitrary state power.’

Norris observed that the two branches of legislature and executive are almost “a complete fusion” because of the existence of parliamentary executives in the UK. Despite this, each branch still has limited "control" and supervision of the operation of

772 Ibid.
773 P Norris, Driving Democracy: Do Power Sharing Institutions Work? (Cambridge University Press 2009) Ch 6. The phrase denotes the fact that the government (i.e. the executive) are part of Parliament (either the House of Commons or the House of Lords).
774 Members of the government, by convention, are members of either House of Parliament (as to the 'near complete fusion', see W Bagehot, The English Constitution (Oxford 2001) 65.
another branch. Therefore, although a government with an absolute majority in the House of Commons may be able to pass legislation relatively easily,\textsuperscript{775} the Parliament still scrutinises this process and can review and reduce excessive executive demands.\textsuperscript{776}

It is important for the Parliament to scrutinise and supervise the actions of the Home Office. The requirement that the Home Secretary keep Parliament informed has been enshrined in some of the terrorism-related executive measures.\textsuperscript{777} In practice, these reports to Parliament, together with the concomitant “annual reviewal” debates, and debates on the introduction of new terrorism-related legislation, have served as the principal ways for Parliament to maintain control.\textsuperscript{778} The parliamentary oversight mechanism mainly includes legislative scrutiny and post-legislative scrutiny.

(1) Legislative scrutiny

The steps required in the process of a bill becoming a parliamentary act offer many opportunities for scrutiny.\textsuperscript{779} Generally, Elliot and Thomas stated that ‘better scrutiny produces better legislation.’\textsuperscript{780} Parliament can review both the legitimacy of the policy and the clarity of the technical language used. It should consider some benchmarks of scrutiny, such as compatibility with the ECHR and the overall clarity and impact of the precise terminology used. However, the effectiveness of parliamentary scrutiny is subject to numerous limitations such as the ability of its members and the dominance of government. The former Chair of the House of Commons Public Administration Committee claimed that the legislative process lacks effective scrutiny because government firmly controls the entire process.\textsuperscript{781}

\textsuperscript{775} ‘the balance of advantage between Parliament and Government in the day to day working of the Constitution is now weighted in favour of the government to a degree which arouses widespread anxiety’ \textit{House of Commons Select Committee on Procedure} (HC 588-1, 1977) viii.
\textsuperscript{776} For specific terrorism-related examples, see e.g. extensions to pre-charge detention limits.
\textsuperscript{777} For the control order obligation, see s. 14(1) Prevention of Terrorism Act 2005; for the obligation of review under the previous powers of preventive detention, see s. 122 Anti-Terrorism, Crime and Security Act 2001; for the requirement of the Home Secretary of State to lay before Parliament the report of the Independent Reviewer on the operation of Terrorism Prevention and Investigation Measures, see s. 20(5) TPIM Act 2011.
\textsuperscript{780} M Elliot and R Thomas, \textit{Public Law} (OUP 2011) 188.
\textsuperscript{781} T Wright, \textit{British Politics: A Very Short Introduction} (OUP 2003) 89.
In order to respond to a terrorism-related emergency or threat, the time allocated for parliamentary scrutiny is inevitably reduced. The House of Lords Constitution Committee has recommended that fast-tracked legislation should usually be subject to a sunset clause, that early post-legislative scrutiny should be the norm, and that the Government should explain to Parliament why a fast-tracked procedure is being sought in the first place.  

The House of Lords is an important bastion against executive power. Usually, there are many experienced experts in various fields who can perform forensic examinations on legislative scrutiny issues. In the context of countering terrorism, for example, Baroness Eliza Manningham-Buller, former Director General of the Security Service, was vociferous in her criticism of the potential extension of pre-charge terrorism detention.  

Another form of legislative scrutiny comes from the work of select committees. The role of such committees in the context of counter-terrorism legislation is vital. For instance, the Joint Committee on Human Rights (JCHR) has provided reports on a panoply of terrorism-related powers, including indefinite detention, pre-charge detention, and control orders. These reports often inform debate in Parliament during the passage and/or renewal of relevant provisions and therefore can influence voting in the House, perhaps against the government. The reports of the

---

783 See for example, the House of Lords’ rejection of 42 days’ terrorist detention; see also Hansard HL Deb 8 July 2008, vol 703, col 647.
784 House of Commons Standing Order 152B.
788 See, for example, the government’s defeat with regard to the proposed extension to pre-charge detention beyond 42 days, following the report of the JCHR (JCHR, *Nineteenth Report of Session 2006-07, Counter-Terrorism Policy and Human Rights: 28 days, intercept and post-charge questioning* (HL 157 HC 394, 2007)).
independent reviewer provide a valuable additional resource that informs the work of the relevant committees.\(^{789}\)

(2) Post-legislative scrutiny

Terrorism-related legislation is subject to parliamentary review once enacted, which is known as post-legislative scrutiny. The committees may be required to report on the legislation’s implementation within one or several years after its enactment in order to re-evaluate its effectiveness and impact. While a 3-5 year review of legislation was established in 2008,\(^{790}\) this is unsuitable when it comes to some counter-terrorism regimes given the pace of legislative change: there have been eight substantive counter-terrorism statutes passed since 2000.\(^{791}\) The role of the independent reviewer is crucial, as the annual reports may provide the basis for the committees’ scrutiny. For example, the independent reviewer of legislation, in a detailed report, has indicated that the definition of terrorism remains broadly fit for purpose, not least because terrorism investigations require earlier intervention than conventional criminal investigations.\(^{792}\)

6.5 Judicial Independence

Both China and E&W have embraced the principle of judicial independence but, in practice, their understandings of judicial independence is quite different.\(^{793}\) In E&W, the judicial independence is driven from the principle of the rule of law and the separation of powers. In the field of anti-terrorism, the judiciary has the power to review anti-terrorism legislation and whether executive agencies have abused their power to violate civil rights.\(^{794}\) In contrast, in China, the judiciary has not been granted power to review anti-terrorism legislation and to supervise the terrorism designation and control

\(^{789}\) See, for example, JCHR, *Counter-Terrorism Policy and Human Rights (Ninth Report)* (HL 57 HC 356, 2007); JCHR, *Counter-terrorism Policy and Human Rights (Sixteenth Report)* (HL 64 HC 395, 2010).

\(^{790}\) House of Commons, *Post-Legislative Scrutiny: The Government’s Approach* (Cm 7320, 2008).


\(^{792}\) Lord Carlile, *The Definition of Terrorism* (Cmd 7052, 2007) 48. Note that the government did not adhere to all of Lord Carlile’s recommendations.

\(^{793}\) The details of “lack of judicial independence” in China could be found in Chapter 4.

\(^{794}\) The details could be found in Chapter 7.
order process.\textsuperscript{795} Therefore, it is arguable that the legal response to cyberterrorism in China has substantially diverged from that of E\&W and that the lack of judicial independence from the executive is a key factor explaining this divergence.

The independence of the judiciary from executive and legislative power is a principle that was established long ago by E\&W's Constitution. The Government does not criticise and/or intervene in the judiciary's decisions.\textsuperscript{796} This used to be a constitutional convention, but it has recently been legally affirmed: ministers have an obligation to ensure the "continuous independence" of the judiciary.\textsuperscript{797} In view of the fact that the executive and legislative branches may limit rights and freedoms in the name of national security, and that the courts have a responsibility to protect human rights and fundamental freedoms from their mixed influence, the independent judiciary in E\&W is very important.\textsuperscript{798}

Courts were reviewing executive action long before the Human Rights Act (HRA) entered into force in 1998. According to Lord Philips, prior to the HRA, the courts deployed the Wednesbury reasonableness test, but under the HRA the courts deploy a proportionality assessment when human rights considerations are in play.\textsuperscript{799} In addition, the HRA strengthens the rule of law and judicial review, and incorporates the principal requirements of the ECHR into the domestic law.\textsuperscript{800} The courts will strive to offer an interpretation of a statute which ensures its compatibility with the UK's obligations under the ECHR.\textsuperscript{801} However, if it cannot interpret a statute in such a way, then it will issue a declaration of incompatibility.\textsuperscript{802}

Judicial review represents the greatest overlap between the judicial and executive departments in terms of control and function. At all instances, the court must be particularly vigilant to ensure that a government does not exceed their legal authority and guarantee their citizens' rights to the greatest extent. In other words, the role of the court is to protect the rights of individuals from the illegal actions of a government.

\textsuperscript{795} The details could be found in Chapter 5.
\textsuperscript{797} s. 3 Constitutional Reform Act 2005.
\textsuperscript{798} RH Wagstaff, \textit{Terror detentions and Rule of law: US and UK perspective} (Oxford University Press 2014) 128.
\textsuperscript{800} Slapper G, Kelly D, \textit{The English legal system} (13th edn, Routledge 2012) 45 .74.
\textsuperscript{801} S 3 of HRA 1998.
\textsuperscript{802} S 4(2) of HRA 1998.
or public institutions. Chapter 7 assesses some court decisions, which have determined whether certain anti-terrorism laws were in compliance with human rights laws and ultimately led to legislative changes. For instance, in the Belmarsh case, indefinite detention was abolished by the House of Lords in 2005. This emphasises the importance of the judiciary’s checking and balancing of the legislator in the context of countering terrorism.

In this realm, the Home Secretary is granted the power to issue a certificate to confirm an individual as a suspected foreign terrorist and to impose a control order or Terrorism Prevention and Investigation Measures (TPIM). In these circumstances, the Home Secretary has extensive discretion and its decisions will be subject to judicial review. Pertinently, Lord Hope recently stated: ‘the rule of law enforced by the courts is the ultimate controlling factor on which our constitution is based,’ and this is an empty principle if it ‘fails to constrain overweening power’. Therefore, the best way to comply with the rule of law is to ensure that administrative discretion is subject to effective judicial review.

The court can review a judgment to see: if the power has been exercised for improper purposes; if the executive member made a legal error in exercising their discretion; whether there is unauthorised decentralisation; whether the policy affects discretion; or whether it violates natural justice or procedural irregularly. Judicial review on the basis of proportionality is of particular relevance to the current terrorism-related paradigms. The main challenges to the detention, control and criminalisation of terrorists all have their roots in the doctrine of human rights.

---

803 This protection is now provided for in ss. 6-7 Human Rights Act 1998.
805 S 1 of PTA 2005.
806 R (Jackson) v Attorney-General [2006] 1 AC 262, [107] (Lord Hope).
807 R (Corner House Research and another) v Director of the Serious Fraud Office [2008] EWHC 714 (Lord Justice Moses).
810 Not likely in a terrorism-related context: Lavender & Son Ltd v Minister of Housing [1970] 3 All ER 871.
812 See, for example, Ridge v Baldwin [1964] AC 40.
813 s. 6(1) HRA 1998 makes it unlawful for a public body to act in a way which is incompatible with an ECHR right; and by s. 6(3)(1)(c) this includes any court or tribunal (thus requires SIAC, as well as the traditional courts, to take account of ECHR rights in the context of terrorism-related challenges).
The judiciary eventually abolished indefinite detention without trial (ATCSA 2001) and control orders (PTA 2005) on the grounds of human rights. Meanwhile, human rights legislation provides clear reasons for the judiciary to exercise control over the use of counter-terrorism power by the executive branch. However, the independent reviewer takes a positive attitude to this judicial intervention, and argued that '[court] judgments have in a number of respects affirmed the importance of liberty and due process without, so far as I can judge, causing an unacceptable increase in the level of risk.'\textsuperscript{813} Even government ministers have recognised the importance of maintaining the rule of law in the face of terrorist threats, and conflict between the executive and the judiciary in this area is inevitable.\textsuperscript{814}

6.6 Basic Criminal Law Principles in E&W

Criminal law plays an important role in dealing with terrorism in E&W, which relies primarily on criminal law to combat the threat of cyberterrorism. In addition, E&W’s legal response to cyberterrorism, via criminal law, is underpinned by a particular conception of the rule of law. This conception emphasises principles such as legality, non-retroactivity, proportionality, maximum certainty, and minimalism. To reinforce this, E&W courts can judicially review executive decisions/actions to ensure compliance with the rule of law.

Therefore, in this section, it is necessary to explain these basic criminal law principles in E&W and how they matter when it comes to fighting terrorism. The role of criminal law principles is a complex one and includes some overlap.\textsuperscript{815} These basic criminal law principles and their use in assess cyberterrorism-related offences will be elaborated below.

6.6.1 The Principle of Legality

\textsuperscript{813} D. Anderson QC, \textit{The Terrorism Acts in 2011} (The Stationery Office 2012) para 11.5.
The principle of legality is derived from the conception of the rule of law outlined above. It implies that no-one should be held criminally accountable and punished without first enacting the law. The aim of this principle is to prevent arbitrary power. Husak derived four subsidiary conditions: ‘(a) laws must not be vague; (b) the legislature must not create offences to cover wrongdoing retrospectively; (c) the judiciary must not create new offences; and perhaps and (d) criminal statutes should be strictly construed.’

Under the case of Beghal v DPP, regarding the question of legality, the Court noted that ‘the law must be adequately accessible to the public and that its operation must be sufficiently foreseeable, so that people who are subject to it can regulate their conduct.’ However, the law must go beyond this ‘to contain sufficient safeguards to avoid the risk that power will be arbitrarily exercised and thus that unjustified interference with a fundamental right will occur.’

This fundamental principle has both procedural and substantive meanings. It expresses respect for the principle of autonomy, which is an undisputed minimum requirement: citizens must be informed of the law before they can be fairly convicted, and both legislatures and courts must apply the rule of law by not criminalising conduct that was lawful when performed. Therefore, the terrorism-related offences must be previously declared, and then people can predict whether their actions will violate the law. This is especially true in the context of combating cyberterrorism.

The principle of legality and its requirements of clarity and precision in offences are non-derogable even in times of public emergency. In this regard, the UN Human Rights Committee has frequently criticised the vagueness of various national terrorism laws in monitoring compliance with the International Covenant on Civil and Political Rights (ICCPR). The UN High Commissioner for Human Rights has summarised

---

817 *Beghal (Appellant) v Director of Public Prosecutions (Respondent)* [2015] UKSC 49, p. 2, para 1 and 6, para 12.
818 Ibid.
819 UN Commission on Human Rights, ‘General Comment No. 29: States of Emergency (Article 4)’ (31 August 2001) UN Doc CCPR/C/21/Rev.1/Add.11, para. 7.
many such concerns as follows: '(1) vague, unclear or overbroad definitions of terrorism led to inappropriate restrictions on the legitimate exercise of fundamental liberties; (2) including non-violent activities in their national definitions of terrorism; (3) defining offences related to supporting terrorism acts must be taken care in case of inadvertently criminalized.'

All of these actions appeared to contravene the principle of legality.

6.6.2 The Principle of Proportionality

The principle of proportionality is to properly limit rights when necessary. No-one, even a criminal, should sacrifice their own interests unless it is absolutely necessary and reasonably proportionate to the harm committed or threatened. A sharper formulation of this principle would be that the principle of necessity, in cases of conflicting rights, grants the authority to inflict only minimum harm. Indeed, the principle of proportionality restricts the extent to which the state can interfere with the rights of individuals.

In the circumstances of countering terrorism, it is widely believed that it should be based on the rhetoric of “balance,” which is also understood as the principle of proportionality: the state must balance individual rights against the need to maintain national security and public safety. Alternatively, the concept of “balance” originates from universal human rights concerns: ‘the public has basic freedoms and can carry out daily business without terror, so the state must balance the rights of the many

---

822 A Ashworth and J Horder, Principles of Criminal Law (7th edn, Oxford University Press 2013) 85.
against the rights of the few.824 These two conflicting and competing interests stem from the protection of the individuals’ right to life enshrined in Article 2 of the ECHR, but at the same time obliges the state to actively protect the lives of those people in its jurisdiction.825 There is, however, a “perilous dichotomy” evident: 826 the threat of terrorism may lead to the defence of the security of some by sacrificing the liberty of others.827 Such balance can lead to inequality, with a minority disproportionately suffering negative consequences.828 The “balance” rhetoric implies a simple direct transaction of one right and another (i.e. achieving a certain finite degree of security at the expense of the specific human rights of the suspected terrorist). For instance, Lord Lloyd asserted, as a guiding principle, that ‘Additional statutory offences and powers ... must strike the right balance between the needs of security and the rights and liberties of the individual.’829 Again, in 2011, in response to the Macdonald Report, the Home Secretary, Theresa May, expressed a determination to:

...correct the imbalance that has developed between the State’s security powers and civil liberties, restoring those liberties wherever possible and focusing those powers where necessary. The review’s recommendations, once implemented, will do this. They will ensure that the police and security agencies have the powers to protect the public and help preserve our cherished freedoms.830

It is generally preferable to recognise that security ‘is a predicate for liberty, not an alternative to liberty.’831 Clive Walker holds the view that ‘the State must accurately make an assessment of anticipatory risk and formulate its legal response in a manner proportionate to that risk; the human rights doctrine of proportionality is central to the quest for constitutional optimisation.’832 According to the CONTEST, which was issued in 2006 and has since been constantly reiterated:

828 Ibid. Thus, Ignatieff argues, disproportionately high numbers of young Muslim males are subjected to restrictions on their liberty; it is not society as a whole that suffers such restrictions.
The protection of human rights is a key principle underpinning our counterterrorism work at home and overseas. A challenge facing any government is to balance measures intended to protect security and the right to life, with the impact on other rights which we cherish. The Government has sought to find that balance at all times.\footnote{Home Office, Countering International Terrorism (Cm 6888, 2006); Home Office, Pursue, Prevent, Protect, Prepare: The United Kingdom’s Strategy for Countering International Terrorism (Cm 7547, 2009); Home Office, Pursue Prevent Protect Prepare: The United Kingdom’s Strategy for Countering International Terrorism (Cm 7833, 2010); Home Office, CONTEST: The United Kingdom’s Strategy for Countering Terrorism (Cm 8123, 2011); Home Office, CONTEST: The United Kingdom’s Strategy for Countering Terrorism (Cm 8583, 2013); Home Office, CONTEST: The United Kingdom’s Strategy for Countering Terrorism (Cm 8848, 2014); Home Office, CONTEST: The United Kingdom’s Strategy for Countering Terrorism (Cm 9048, 2015); Home Office, CONTEST: The United Kingdom’s Strategy for Countering Terrorism (Cm 9310, 2016).}

Some rights are non-derogable, while some rights can be derogable under certain circumstances. According to Article 3 of the ECHR, the right of prohibition of torture and ill-treatment is non-derogable without exception.\footnote{ECHR, Art.3.} Other ECHR rights\footnote{Most notably ECHR, Articles 8-11.} are subject to restrictions as are ‘prescribed by law and are necessary in a democratic society.’\footnote{ECHR, Articles 8(2), 9(2), 10(2) and 11(2).} Essentially, no restrictions on these rights can be considered unless they are commensurate with the goals pursued.\footnote{See generally Y Arai-Takahashi, The Margin of Appreciation Doctrine and the Principle of Proportionality in the jurisprudence of the ECHR (Hart 2001). It may be that future challenges to TPIMS are predicated on the basis of Article 8 ECHR and Article 10 ECHR, but given the qualifications to these rights, successful challenges may be unlikely.} Restrictions on Articles 5 and 6 of the ECHR must be ‘in accordance with law’ and subject to judicial oversight, in accordance with the ECHR’s general protection for the rule of law; proportionality is also a feature of these determinations.\footnote{ECHR, Article 5(1), 5(3), 5(4), Article 6(1). For proportionality in the context of Article 6 ECHR, see Smith and Grady v UK (1999) 29 EHRR 493.}

E&W’s judiciary must apply proportionality in executive decision-making in the context of anti-terrorism strategies. In SSHD v Daley,\footnote{SSHD v Daley [2001] UKHL 26.} the House of Lords imported proportionality as a test to replace the traditional judicial review criterion of reasonableness. The meaning of “proportionality” has been the subject of much judicial dicta, and according to the House of Lords requires that:\footnote{SSHD v Daley [2001] UKHL 26 [2002] 2 AC 532, 547, citing de Freitas v Permanent Secretary of Ministry of Agriculture, Fisheries, Lands and Housing [1999] 1 AC 69, 80.}
(1) the legislative objective is sufficiently important to justify limiting a fundamental right; (2) the measures designed to meet the legislative objective are rationally connected to it; and (3) the means used to impair the right or freedom are no more than is necessary to accomplish the objective.

Alternatively, Elliot and Thomas have summarised the doctrine with reference to four questions regarding to ‘the relationship of proportionality between the damage caused to the protected interest and the achieving the legitimate aim.’

In order to enact a proportionate provision, there are a number of guiding principles to consider. In general, the state should take the necessary restrictive and minimal measures in all circumstances to achieve its legitimate purpose; this is especially true for the scope of terrorism-related offences and the range of control orders and TPIM conditions that may be imposed on individuals.

6.6.3 The Maximum Certainty Principle

Another basic requirement of the rule of law principle is that the law should be certain and clear to the maximum extent. The wording of the law should be as clear as possible so that each individual is aware of their responsibilities and is able to make informed choices about their actions. Narrowly speaking, clearly drawn laws also limit the discretion vested in officials, thus providing protection against inconsistent or inappropriate decision-making by those tasked with implementing the law. This principle aims to promote the rule of law, so it is necessary to consider the reduction of arbitrary powers and the provision of an appropriate degree of legislative authority in the context of existing terrorism legislation. Lord Diplock has stated: ‘absence of clarity is destructive of the rule of law; it is unfair to those who wish to preserve the rule of law; it encourages those who wish to undermine it.’ The counter-terrorism framework should be established and restricted in the form of statutes according to the

---

841 M Elliot and R Thomas, Public Law (OUP 2014) 522; and see Huang v Secretary of State for the Home Department [2007] UKHL 11.
844 Merkur Island Shipping Corporation v Laughton [1983] 2 AC 570, 614 (Lord Diplock).
principle of certainty. The ECtHR’s positive guidance on the interpretation of this principle is as follows.845

A law should be formulated with sufficient precision to enable the citizen to regulate his conduct; he must be able, if need be with appropriate advice, to foresee to a degree that is reasonable in all the circumstances, the consequences which a given action may entail.

Meanwhile, Lord Bingham has captured the essence of this principle: ‘the broader and more loosely-textured discretion is, the greater the scope for subjectivity and hence for arbitrariness, which is the antithesis of the rule of law.’846 The HRA grants the judiciary a certain degree of determination with respect to the meaning of imprecise statutory terms, and there is a natural tension between the power of statutory interpretation and the need for legislative certainty.847

According to the ECtHR, the legal precedent formed during the evolution of the common law system does not conflict with the certainty requirements of Article 7 of the ECHR.848 But the common law system retains the possibility of uncertainty in specific areas.849 In light of this position, ATH Smith has argued for the enactment of a criminal code in order to imbue the legal regime with further certainty.850

Additionally, the principle of maximum certainty has a close relationship with the non-retroactivity principle. An ambiguous law may be retroactively enforced in practice, because no-one can determine whether the given conduct is within or outside the rule. Thus, Article 7 of the Convention is relevant here, and states:

> Not confined to prohibiting the retrospective application of the criminal law to an accused’s disadvantage. It also embodies, more generally, the principle that only the law can define a crime and proscribe a penalty (*nullum crimen, nulla poena sine* ...

---

845 *Sunday Times v United Kingdom* (1979) 2 EHRR 245, [49].
849 For a detailed (and indeed world-renowned) exposition of this concept, see A D’Amato, ‘Legal Uncertainty’ (1983) 71 CLR 1.
lege) and the principle that the criminal law must not be extensively construed to an accused’s detriment, for instance by analogy: it follows from this that an offence must be clearly defined in law. This condition is satisfied where the individual can know from the wording of the relevant provision and, if need be, with the assistance of the courts’ interpretation of it, what acts and omissions will make him liable. 851

However, the Strasbourg Court has also recognised that some vagueness is inevitable in order ‘to avoid excessive rigidity and to keep pace with changing circumstances,’ and that a reasonable settled body of case law may suffice to reduce the degree of vagueness to an acceptable proportion. 852 As the Court stated in the Sunday Times case:

Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a ‘law’ unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able—if need be with appropriate advice—to foresee, to a degree that is reasonable in the circumstances, the consequences which his given action may entail. 853

A related reason for supporting the principle of maximum certainty is that if the rules are drafted ambiguously, they will give law enforcement officials considerable power: the police or other agencies will likely use a wide-scoped crime to criminalise acts not envisioned by the legislature, creating the kind of arbitrariness that according to the values of the rule of law should be avoided.

However, the principle of maximum certainty indicates that the law does not require absolute certainty. In its purest form, the rule of law will entail complete certainty and predictability, but this is seldom achieved as explained by Timothy Endicott: ‘vagueness is ineliminable from a legal system, if a legal system must do such things as to regulate the use of violence...’ 854 As Timothy Endicott argued, neither vagueness nor discretion is necessarily a deficit in the rule of law, so long as the law

853 Sunday Times v UK (1979) 2 EHRR 245, para 49; see generally B Emmerson, A Ashworth and A Macdonald(eds), Human Rights and Criminal Justice (3rd edn, Sweet & Maxwell 2012), ch 16.
can perform its guiding function.\textsuperscript{855} Therefore, adherence to the principle of maximum certainty means that those vague terms should be reinforced by other defining elements, guidelines or illustrative examples which inform the citizen and the court’s discretion.

\section*{6.6.4 The Non-Retroactivity Principle}

The essence of the non-retroactivity principle is that a person should never be convicted or punished except in accordance with a previously declared offence governing the conduct in question.\textsuperscript{856} The core of this principle is that a person should never be convicted or punished of any criminal offence unless there are previously declared offences governing the conduct in question.\textsuperscript{857} Article 7 of the ECHR stipulates the principle of prohibition on criminal retrospectivity and this principle, which is also referred to as the principle of \textit{nulla crimen sine lege} (no punishment without law), stipulates: ‘no one shall be held guilty of any offence on account of any act or omission which did not constitute a criminal offence under national or international law at the time when it was committed.’\textsuperscript{858}

However, the enactment of excessively broad terrorism-related legislations raises a key human rights issue which is also central to the rule of law: the violation of the prohibition on retrospective criminal punishment under Article 7 of the ECHR.\textsuperscript{859} The prohibition on retrospective punishment requires that the crime must be sufficiently certain to enable a person to prospectively understand the range of their legal liabilities. As stated by the ECtHR in \textit{Kokkinakis v Greece}:

\begin{quote}
... the principle requires that the criminal law must not be extensively construed to an accused’s detriment, for instance by analogy; it follows from this that an offence
\end{quote}

\textsuperscript{856} The non-retroactivity principle does not affect the creation of defences to crimes, although the courts have sometimes deferred to the legislature on this matter. For theoretical discussion of this point, see PH Robinson, ‘Rule of Conduct and Principles of Adjudication’ (1990) 57 UCLR 729, and P Alldridge, ‘Rules for Courts and Rules for Citizens’ (1990) 10 OJLS 487. The non-retroactivity principle does not apply to retrospective changes that benefit an accused person: \textit{Scoppola v Italy} (no 2) [GC], no. 10249/03, 17 September 2009.
\textsuperscript{857} Ibid.
\textsuperscript{858} ECHR, Article 7.
\textsuperscript{859} ECHR, Article 7.
must be clearly defined in law. This condition is satisfied where the individual can know from the wording of the relevant provision and, if need be, with the assistance of the courts' interpretation of it, what acts and omissions will make him liable.860

In opposition to the strictness of the principle of non-retroactivity and applicable to the creation of entirely new offences, the ECtHR holds a surprisingly generous view of the extent to which the courts must develop existing crimes to cover new ground.861 According to ECtHR:

Article 7(1) excludes that any acts not previously punishable should be held by the courts to entail criminal liability or that existing offences should be extended to cover facts which previously did not clearly constitute a criminal offence. It is, however, compatible with the requirement of Article 7(1) for existing elements of an offence to be clarified or adapted to new circumstances or developments in society in so far as this can reasonably be brought under the original concept of the offence. The constituent elements of an offence may not however be essentially changed to the detriment of an accused and any progressive development by way of interpretation must be reasonably foreseeable to him with the assistance of appropriate legal advice if necessary.862

With this in mind, the development of the law by E&W courts could adapt legitimately to new circumstances, however the constituent elements of the crime must not be changed substantially so as not to harm the defendant's interests. This decision implants a degree of flexibility into what ought to be a fundamental rule-of-law protection for individuals, making it more compatible with an authoritarian principle.863 Obviously, it has been observed that E&W has expanded existing terrorism-related offences to apply to new circumstances (such as cyberterrorism).

6.6.5 The Principle of Minimalism

860 Kokkinakis v Greece (1993) 17 EHRR 397, para. 52; see also Castillo Petruzzi et al v Peru[1999] IACHR 6 (30 May 1999), para. 121.
863 A Ashworth and J Horder, Principles of Criminal Law (7th edn), Oxford University Press 2013) 87.
The principle of minimalism is one of the most important rule of law values, and relates to the scope of the legislation. Laws should be as narrowly drawn as possible in order to preserve individuals’ autonomy and freedom to choose, to the fullest extent possible. With this in mind, the principles of proportionality and minimalism have a certain degree of overlap. The first key issue of the minimalist approach is that the criminalisation should respect human rights protection. This means that the criminal law should respect freedom of expression, freedom of assembly and association, freedom of thought and religion, the right of privacy, the right to not be discriminated against. However, it does not mean that these rights could not be curtailed or abridged by criminal law in any case. Therefore, it is implied that criminal law could interfere with them if it is ‘necessary in a democratic society’ for one of the stated purposes. Accordingly, the freedom of expression may be curtailed for the offence of sending a grossly offensive message through a public communication system, for offences of speech likely to stir up racial or religious hatred, or for inciting terrorism (s.59 of TA 2000).

Another important point is that criminalisation is a last resort. Husak argued that ‘this demand—often thought to have general application to all criminalization.’ As well as criminalisation, civil liability and administrative regulation are other prominent techniques applied in this regard. Therefore, an assessment should be undertaken to determine whether the misconduct has been appropriately handled firstly by civil liability or administrative responsibility. The key issues of appropriateness here will depend on other factors, such as the public factors in the wrongful act and the severity of the harm or wrong involved. The thrust and application of the principle is that criminal law should be retained as the last legislative instrument and used only for serious wrongful or harmful acts. However, E&W law lacks a general sanctioning system which ‘does not involve the censure of the criminal law—a system of civil violations, infractions, or administrative wrongs.’ This makes it difficult to scrutinise the adequacy of non-criminal sanctions before criminalisation. Otherwise, it may lead to over-criminalisation.

---

866 But note s. 29J of the Public Order Act 1986 (inserted by the Racial and Religious Hatred Act 2006), re-stating freedom of expression as a value.
867 For general discussion, see D Husak, ‘Criminal Law as Last Resort’ (2004) 24 OJLS 207.
868 A Ashworth and J Horder, Principles of Criminal Law (7th edn, Oxford University Press 2013) 64.
The third component of the minimalist approach is ‘the principle of not creating a
criminal offence, or a set of offences, where this might cause greater social harm than
leaving the conduct outside the bounds of criminal law, or where the prohibition is
unlikely to be effective.’ This implies that only if an act is seriously harmful could
criminalisation be justified. The minimalist approach requires that the law’s most
coercive and censuring technique (criminalisation) should be reserved for the most
serious invasions of interests.

6.6.6 The Harm Principle

The essence of the harm principle is that the state is justified in criminalising any
conduct that causes harm to others or creates an unacceptable risk of harm to
others. Its main thrust is as a negative or limiting principle, with the objective of
restricting the criminal law from penalising conduct that is regarded as immoral or
otherwise unacceptable but which is not harmful to others.

Feinberg defined harm as ‘those states of set-back interest that are the consequence
of wrongful acts or omissions of others.’ Given this definition, harm and
wrongfulness are two basic requirements for criminalisation. When it comes to stating
a positive version of the harm principle, Feinberg proposed the following definition: ‘It
is always a good reason in support of penal legislation that it would probably be
effective in preventing (eliminating, reducing) harm to persons other than the actor and
there is probably no other means that is equally effective at no greater cost to other
values.’ Except for the harm, another important element of criminalisation is
wrongfulness. Basically, it is not only the causing of harm that justifies

---

criminalisation, but the wrongful causing of harm (i.e. wrongfully harming other’s interests). Andrew Simester and Andreas von Hirsch developed the argument that one necessary prerequisite of criminalisation is that the conduct amounts to a moral wrong. However, before criminalization is justified, not only must the conduct be morally wrong, but there must also be no strong countervailing considerations, such as the absence of harm, the creation of unwelcome social consequences, the curtailment of important rights, and so forth. In fact, because the consequences of criminal punishment are to restrict or even deprive citizens of their basic rights, the case needs to be particularly strong to restrict the criminalisation of non-serious moral wrongs. However, it does not seem easy to determine whether certain terrorist precursor offences are wrongful acts, such as the offence of the possession of material that may be useful to a person committing or preparing to commit an act of terrorism, as stipulated under s 58 of the TA 2000.

Another kind of justification for criminalisation is remote harms, which means that certain conduct may create an opportunity for serious subsequent harm. The preventive function of criminal law empowers the state to criminalise an act that creates the risk of a certain harm: the act itself may not be harmful or wrongful, but it is criminalised because of its possible consequences. An example here is that the prohibition of conduct based on what the individual may do subsequently (e.g. criminalising the possession of a document, money or other property or collecting information likely to be useful to a terrorist (s 58, s 57, s16 TA2000) and preparation of terrorist acts(s 5 TA2006)). A further example is a prohibition of conduct based on what others may be led to do subsequently (e.g. criminalising the encouragement of terrorism (s 1 TA2006, s 59 TA 2006) and dissemination of terrorist publications (s 2 TA 2006)).

---

879 For a discussion of the difficulties of reconciling possession offences with the general paradigm of criminal law, see A Ashworth, ‘The Unfairness of Risk-Based Possession Offences’ (2011) 5 CLP 237.
There are widespread disputes about whether the risk of harm constitutes harm itself and whether offences targeting the risk of harm contravene the harm principle.\textsuperscript{881} Criminal law could be used to prevent the risk of harm in certain defined situations.\textsuperscript{882} However, the objection to the criminalisation of remote harms is based on the grounds that ‘criminal responsibility should not be borne for the act that is not harmful in itself, or (as with the inchoate offences) at least not unless it is accompanied by an intention to encourage, assist, or commit a substantive offence.’\textsuperscript{883} This would rule out most possession offences without any evidence of further intent. Specifically, situations where the occurrence of the harm depends on the further decision of the actor or another actor are not suitable for criminalisation.\textsuperscript{884} This is, of course, a restriction on liberty. Therefore, when contemplating whether there is a justification to curtail liberty, the severity of the harm and the possibility of its occurrence should be taken into account.

The Terrorism Act 2006 (TA 2006) contains offences that extended the ambit of the criminal law.\textsuperscript{885} How could the harm principle set out here apply to these offences? A good example here is the offence of publishing a statement that is likely to be understood as glorifying acts of terrorism, intending to encourage others or reckless as to whether others are encouraged to commit or prepare for such acts.\textsuperscript{886} Some characteristics of this offence are related to the harm principle. First, it is an inchoate offence aimed at preventing remote harm (e.g. there is no requirement that anyone is encouraged, let alone that anyone actually carries out, any of the preparatory acts mentioned (s. 1(5)(b))). Those acts would, based on traditional principles, be the responsibility of the person carrying them out (although the encourager would also be liable).\textsuperscript{887} Secondly, the offence does not require proof of an intention to encourage the commission of these further acts: recklessness is sufficient. For instance, it is

\textsuperscript{881} D Husak, \textit{The Philosophy of Criminal Law} (Oxford University Press 2010) 127. See also John Oberdiek, ‘Towards a Right Against Risking’ (2009) 28 LP 367; for an argument in favour of a ‘right against risking’ that is grounded in the interest in autonomy, and C Finkelstein, ‘Is Risk a Harm?’ (2003) 151 UPLR 963, where it is argued that a risk constitutes a harm, based on the argument that minimizing risk exposure is an ‘element of an agent’s basic welfare’.

\textsuperscript{882} J Feinberg, \textit{Harm to Others} (Oxford University Press on Demand 1984) 216.


\textsuperscript{884} For further discussion, see A Ashworth, ‘The Unfairness of Risk-Based Possession Offences’ (2011) 5 CLP 237; A Ashworth, \textit{Positive Obligations in Criminal Law} (Bloomsbury Publishing 2013) ch 6.

\textsuperscript{885} See the analysis by V Tadros, ‘Justice and Terrorism’ (2007) 10(4) NCLR 658.

\textsuperscript{886} TA 2006, S 1(2).

\textsuperscript{887} See the offences of ‘encouraging and assisting crime’ introduced by Part 2 of the Serious Crime Act 2007.
sufficient as long as the statement is ‘likely to be understood by some members of the public’ as an encouragement (s. 1(1)) and if members of the public ‘could reasonably be expected to infer that what is being glorified is being glorified as conduct that should be emulated by them in existing circumstances’ (s. 1(3) (b)). Unlike other inchoate offences, the proof of intent is not required for this offence. Therefore, the harm principle is broad enough to accommodate the criminalisation of acts risking harm, not because the acts are harmful per se, but because the harm principle focuses on preventing harm.

The harm principle represents a significant element of liberal versions of criminal law. The harm principle implies that the immorality alone is not a sufficient requirement for criminalisation, and that rather conduct may only justifiably be criminalised if it wrongfully causes harm to others. However, these offences must cause substantial damage, for example, the death or injury of the victim, or the actual occurrence of an explosion or kidnapping. In addition, the criminal law also contains the inchoate offences of attempt, conspiracy and encouraging crime. According to Horder, these offences imply that the criminal law also has a preventive function. As Ashworth and Zedner have observed: ‘If a certain form of harmful wrongdoing is judged serious enough to criminalize, it follows that the state should assume responsibility for taking steps to protect people from it’.

Although there have been some well-known convictions for inchoate offences in terrorism-related cases, there are still many challenges in judicial practice. Obviously, the crimes of conspiracy and encouragement or incitement are difficult to prove. It is difficult to obtain acceptable evidence of an agreement or words of

---

888 A Ashworth and J Horder, Principles of Criminal Law (7th edn, Oxford University Press 2013) 69.
889 Tadros argues that the Harm principle ‘must be understood to include conduct that creates a risk of harm or a tendency to harm’ and is thus fairly broad. V Tadros, ‘Crimes and Security’ (2008) 71(6)MLR 940, 942; Simester and Von Hirsh state that “in the absence of harm, or risk of harm, the state is not normally entitled to intervene”. AP Simester and AV Hirsch, Crimes, Harms, and Wrongs: on the Principles of Criminalisation (Hart Publishing 2011) 35.
892 Abu Hamza’s conviction for soliciting to commit murder and the convictions of seven men on conspiracy charges in the airline liquid bomb plot case. Three of the men (the ringleader, his right hand man and the explosives expert) were convicted of conspiracy to murder aircraft passengers using explosives. The other four (the would-be suicide bombers) were convicted of conspiracy to murder. See R v Ali (Ahmed) & others [2011] EWCA Crim 1260.
encouragement within a secret organisation, especially given the circumstances in which the UK prohibits the use of interception as evidence. Moreover, even if admissible evidence is obtained, it may lack evidentiary value (for example, members of a terrorist organisation cover up their communication content) or the information cannot be disclosed for reasons of public interest.\footnote{Home Office, \textit{Privy Council Review of Intercept as Evidence: Report to the Prime Minister and the Home Secretary} (Cm 7324, 2008).}

There is a limited scope of attempt crimes which were governed by criminal law. In such crimes, the offender commits the offence of attempting which is ‘more than preparatory to the commission of the full offence.’\footnote{Criminal Attempts Act 1981, s 1(1).} However, due to the level of risk and severity of the potential harm in the context of terrorism-related offences, it is strongly necessary to penalise acts at an early stage. In the words of the independent reviewer of terrorism legislation, Anderson QC, it is necessary to ‘defend further up the field,’\footnote{D Anderson QC, ‘Shielding the Compass: How to Fight Terrorism Without Defeating the Law’ (2013) SSRN 1-19 <https://ssrn.com/abstract=2292950> accessed 10 Oct 2020.} This is the preventive function of precursor—or pre-inchoate—offences. Therefore, the satisfaction of the harm principle is a justification for the criminalisation of terrorism precursor offences. However, an overbroad range of terrorism precursor offences that may cause harm to some degree could contravene the harm principle, which need sufficiently powerful constraint on criminalization.

\textbf{6.6.7 The Principle of Normative Involvement}

E&W has criminalised a wide range of terrorism precursor offences, largely found in the Terrorism Acts 2000 and 2006.\footnote{Details could be found in Chapter 7.} Simester and von Hirsch have proposed the principle of normative involvement to keep the realm of precursor offences within an appropriate range. Many ancillary cyberterrorism activities penalised by the precursor offences—such as collecting information, possessing items, or raising funds—will not themselves cause harm to others. Harm is only caused when the perpetrator subsequently chooses to act in a particular manner. According to the principle of normative involvement, if the defendant ‘in some sense affirms or under-writes’ this subsequent choice he may justifiably be penalised for his preparatory acts.\footnote{AP Simester and AV Hirsch, \textit{Crimes, Harms, and Wrongs: on the Principles of Criminalisation} (Hart Publishing 2011) 81.} He...
recognised that the offender should take responsibility for potential future harm caused by future harmful actions. The principle of normative involvement not only justifies the creation of precursor offences, but also limits their range.

If normative involvement limits the scope of precursor offences in principle, then some of the existing offences will fall outside this scope. A good example here is the use of the Internet to collect information or possess documents likely to be useful to a terrorist (s 58 of TA 2000). Individuals may be convicted of this crime even without any normative involvement in a terrorist conspiracy. This could be demonstrated by the case of *R v G*.898

Since the s 58 of the TA 2000 does not specify the mens rea of the perpetrator, it leaves the offender a reasonable possibility to avoid conviction. There are two mental elements required of the offence: first, the defendant must have known that he had possession or control of the document; and, second, he must have been aware of the nature of the information contained therein. However, these requirements alone are not sufficient enough to establish any normative involvement in terrorist activity. Therefore, the accused may satisfy these requirements even though he has no intention of committing terrorism. So, in the case of *R v G*, the key question was whether the Court of Appeal’s interpretation of the reasonable excuse defence was correct or not. The House of Lords held that G’s defence was not reasonable and thus unavailable to him.

6.7 Conclusion

This thesis aims to figure out whether the rule of law in E&W or “rule by law” in China produces markedly different legal responses to cyberterrorism. In order to achieve this purpose, it is relevant to map out the distinctive characteristics of the legal regime in the E&W, which is based on the rule of law, separation of powers and judicial

898 K v R [2008] EWCA Crim 185. ‘The defendant in this case was a paranoid schizophrenic. He had been detained for a number of non-terrorism offences. While in custody he collected information on explosives and bomb-making, and also drew a map of the Territorial Army centre in Chesterfield and wrote down plans to attack the centre. The items were discovered during a search of his cell. He was charged with collecting information of a kind that was likely to be useful to a terrorist under section 58 of the Terrorism Act 2000. His explanation for collecting the information was that he wanted to wind up the prison staff because he believed they had been whispering about him. He said ‘I wanted to wind them up and I know how this terrorism stuff ... really gets on their nerves’.
independence. In order to conduct a critical comparative analysis of legal approaches to cyberterrorism between the PRC and the UK, it is significant to explore the legal principles underlying their legislation which could help to further explain the convergences and divergences between them.

The ensuing description highlighted the relevance of a number of rule-of-law principles, including maximum certainty, proportionality, non-retroactivity, minimal criminalisation, and harm, which raises a variety of questions for the next chapter. These questions include: “How can E&W's existing terrorism legislation be applied to combat the threat of cyberterrorism?”; and “Is there a risk that E&W's existing counter-terrorism strategy and framework could lead to rule by law rather than the rule of law?” The rule of law contrasts with arbitrary power while, rule by law, on the other hand, involves cloaking arbitrary power in legal form.899 Therefore, although E&W's legal regime is based on the rule of law, does it have some rule-by-law tendencies in the context of cyberterrorism? All of these questions will be investigated in subsequent chapters.

Chapter 7 Legal Responses to Cyberterrorism in E&W

7.1 Introduction

Similar to the situation in China, no law is specifically devoted to countering cyberterrorism in E&W. Instead, the latter relies on existing anti-terrorism laws to combat cyberterrorism.\textsuperscript{900} The UK government aims to build on existing laws to fill gaps and close perceived loopholes. This chapter aims to comprehensively analyse and critically evaluate the existing laws in terms of the basic principles elaborated upon in the last chapter.

Firstly, I start with E&W’s pre-emptive and preventive tendencies in its legal responses to cyberterrorism. In the comprehensive counter-terrorism strategy CONTEST, the pre-emptive and preventive measures and the reduction of anticipatory risk and proactively combating terrorism are all highlighted. Moreover, based on the rule of law, it broadens the boundaries of the traditional criminal justice system, manifested in the proliferation of precursor criminal offences, and the granting of broad executive powers to investigate, detain and control suspected terrorists.

Secondly, similar to China, although E&W tends to give priority to national security in its anti-terrorism policy and substantive laws, there appears to be a certain amount of balancing between collective security and individual rights protection upon closer examination of E&W’s pre-emptive measures in judicial practice. In other words, there is a huge difference in the anti-terrorism practices of China and E&W, driven by the role and importance of judicial review, judicial independence and the over-arching scrutiny provided by commissioners and parliamentary committees in the latter.

Thirdly, like China, there is no specific definition of cyberterrorism in E&W’s anti-terrorism laws, with the definition of terrorism in the Terrorism Act 2000 relied upon instead. It has been argued that vague or over-inclusive definitions raise serious

concerns about violating the principles of legality and certainty, and result in arbitrary judicial application. In addition, a wide-reaching definition of terrorism serves to further extend the reach of the criminal law and permit overbroad discretion when it comes to designating terrorists.

Fourthly, similar to China, E&W has criminalised a wide range of preparatory or inchoate terrorism offences to address the ancillary activities, which hang off the primary definition of terrorism. Crucially, the imprecision of counter-terrorism laws contravene the principles of legality and minimal criminalisation. These preparatory or inchoate offences include group-based offences, speech-related offences and supportive terrorism-related offences. The rationale behind criminalising such offences is to capture the potential acts of anticipatory risk, and this may violate the principle of minimal criminalisation. Moreover, such offences also carry harsh punishment, which could violate the principle of proportionality, suggesting, in turn, that E&W has utilised a punitive strategy in response to the threat of terrorism. In addition, the executive organ is granted broad discretion to designate proscribed terrorism organisations, but the role of the judiciary in the proscription process is limited.

Fifthly, with respect to the enforcement of anti-terrorism measures, it could be observed that the executive has been granted broad powers to investigate, detain and control suspected terrorists, including the expansion of pre-trial detention, overbroad stop-and-search powers, extensive discretion to issue control orders and TPIMs, and the application of non-criminal disruption methods to deal with preparatory cyberterrorism acts.

7.2 Preventive and Pre-emptive Tendencies

Similar to China, E&W has preventive and pre-emptive tendencies in its legal responses to cyberterrorism, as demonstrated in its policy, substantive laws and practical enforcement thereof.
From the political perspective, the UK government first published a clear and comprehensive counter-terrorism strategy called CONTEST in 2006, and it has since undergone many revisions. The strategy contains the “4Ps” work strands which are as follows:

1. Pursue: to stop terrorist attacks
2. Prevent: to stop people becoming terrorists or supporting terrorism
3. Protect: to strengthen our protection against terrorist attack
4. Prepare: to mitigate the impact of a terrorist attack

CONTEST aims to pre-emptively reduce the risk of terrorism, so that people can go about their normal lives, freely and with confidence. It places an emphasis on reducing anticipatory risk and proactively combating terrorism to prevent large-scale casualties to the maximum extent possible. It is then necessary to stop would-be perpetrators before a terrorist act is committed. Therefore, based on the rule of law, the boundaries of the traditional criminal justice system are broadened, manifested in the proliferation of precursor criminal offences, the repealing of the section 44 stop-and-search powers and replacing these with more limited powers, and abolishing control orders and replacing with TPIMs. Although Walker criticised some administrative measures for being excessive, he also admitted that they were an integral part of the CONTEST strategy. He noted that the nature of the potentially devastating effect of terrorism requires the application of ‘all-risk security and policing

---

901 Home office, Countering International Terrorism: the United Kingdom’s Strategy (Cm6888, 2006).
902 For example, the CONTEST strategy was revised by the Brown government in March 2009 and again by the Coalition government in July 2011.
905 Home Office, The United Kingdom’s Strategy for Countering International Terrorism (Cm 7547, 2009) 5
measures, such as stop-and-search powers.\textsuperscript{912}

Many scholars have identified a shift in criminal law towards a pre-emptive paradigm in the post 9/11 era.\textsuperscript{913} In particular, terrorism seems to have become a justification to extend precautionary and pre-emptive principles into the political arena.\textsuperscript{914} Even prior to 9/11, Ericson, Haggerty and Walker argued that the UK’s anti-terrorism policy had shifted from reactive to proactive, especially in terms of policing and risks management.\textsuperscript{915} Beck and Walker meanwhile held that pre-emptive measures run through the UK’s anti-terrorism legal framework to deal with anticipatory risks.\textsuperscript{916} In addition, Aradau and van Munster cogently argued that the precautionary principle is conducive to rapid government decisions to combat terrorism.\textsuperscript{917} However, Hudson argued that the adoption of such a principle raises concerns about due process and proportionality.\textsuperscript{918}

(2) From the substantive law perspective, for CONTEST to achieve its goal, E&W has developed a wide range of “precursor crimes” to allow for early intervention against terrorist threats without having to wait the conclusion of an outrage.\textsuperscript{919} In order to combat the proliferation and destructiveness of terrorist attacks, early state intervention is considered essential.\textsuperscript{920} Pertinently, Borgers and van Sliedregt

\textsuperscript{912} C Walker, ‘Neighbor Terrorism and the All-Risk Policing of Terrorism’ (2009) 3 JNSLP 121, 130.
\textsuperscript{918} B Hudson, Justice in the Risk Society (Sage Publications 2003).
\textsuperscript{919} C Walker and M Conway, ‘Online terrorism and online laws’ (2015) 8(2) DAC 156, 163.
\textsuperscript{920} For attack on Turkey, see A Ansari and G Tuysuz, ‘Ankara car bomb explosion kills 34; Turkey
identified the following four preventive characteristics of anti-terrorism legislation:

1. Criminalising the preliminary stage of the offence;
2. Expanding investigative powers;
3. Expanding pre-trial detention; and
4. Using non-criminal measures to achieve a repressive effect.  

The basic rationale behind the forward-looking preventive counter-terrorism legislations was ensuring public safety and security from the terrorist threat. This approach has the potential to forestall ‘risks, [and] competes with and even takes precedence over responding to wrongs done.’ For example, the TA 2000 includes several trigger offences that extend inchoate liability, including s 57 (possession of an article for terrorist purposes) and s 58 (collection of information useful for an act of terrorism), which together have resulted in the highest proportion of charges under counter-terrorism legislation. This is in line with the UN Security Council Resolution 1373, which requires that all states must criminalise the serious acts of planning, financing, preparation or perpetration of terrorism in domestic law and that the punishment should reflect the seriousness of such acts. However, Walker has claimed that pre-emptive laws should not be adopted in non-crisis period.

---


925 UNSC, Res 1373(28 Sep 2001) UN Doc S/RES/1373, s 2(e).
During the House of Commons debate on the proposed TA 2006, the following statement was made about justification for early intervention based on public safety is evidenced in the following statement: 'The need to ensure public safety by preventing such attacks means that it is necessary to make arrests at an earlier stage than in the past, where there was a culture of warning and where weapons of mass destruction did not exist as now.'

The offences extending inchoate liability in the TA 2000 and the TA 2006 seek to criminalisation any acts that may lead to future harm or have the potential risk of perpetration of future harm. The criminalisation of acts that enable future harm is a reflection of the preventive nature of recent criminal legislation in E&W. These risk-based offences rely on forward-looking preventive rationales for their legitimacy. The UK government offers arguments based on security and on the state’s duty to protect the public (or the state itself) from harm to justifying these measures. According to Ashworth, criminal law has a preventive function, meaning the prevention of future acts of culpable wrongdoing. So, prevention is a legitimate goal of criminal law because one of the state’s responsibilities is to ensure public safety and to protect the public from harm. However, states have other responsibilities, particularly in liberal democracies such as E&W, including the maintenance of various liberties such as innocence until proof of guilt, on the facts, after the facts and beyond all reasonable doubt before any circumscription of individual liberties can be justified. A core tension here arises between these multiple responsibilities and how to resolve clashes between rival responsibilities, such as public protection and due process. Perceived failures to resolve conflicts between these responsibilities have been central to the

---

927 HC Deb 26 Oct 2005, col 344.
928 Inchoate offences being those of assisting and encouraging primary offences.
930 See D Feldman, ‘Human rights, terrorism and risk: the roles of politicians and judges’ (2006) 2PL 364 at 369, quoting from the briefing paper Three Month Pre-Charge Detention prepared by the Anti-Terrorist Branch of the Metropolitan Police, SO13, and sent to the Home Secretary by Assistant Commissioner of the Metropolitan Police, Mr. Andy Hayman QPM, MA, on 6 Oct 2005: ‘public safety always comes first, and the result of this is that there are occasions when suspected terrorists are arrested at an earlier stage in their planning and preparations than would have been the case in the past.’
931 The need to recognize the preventive function (of the criminal law) as one of the central functions of the criminal law is not in doubt; it would not make sense if the criminal law were purely a retrospective, blaming institution, since the seriousness with which it treats wrongs against physical safety, for example, points to the importance of preventing those wrongs from occurring. This supplies the rationale for the inchoate offences and, less strongly, for many of the possession offences.
criticisms of CONTEST, especially the preventive strand and its several revisions over the past decade.

(3) From the practical perspective, E&W's strategy became the driving force to provide state and law enforcers with powers to prevent terrorism as part of a security response.932 For example, the TA 2000 and subsequent anti-terrorism laws, including non-criminal disruption measures, aided in establishing an era of countering terrorism predominantly based on pre-emptive and preventive measures. A prominent example of these pre-emptive counter-terrorism measures is the control order scheme, which will be analysed in detail below.933

7.3 Balancing Terrorism Prevention and Human Rights Protection

Although pre-emptive and preventive measures have become the basis for the counter-terrorism strategy in E&W, due consideration still needs to be given to protecting the rights of individuals to comply with the rule of law. The protection of human rights has thus become a core part of CONTEST.934 How to balance security and freedom in the context of counter-terrorism has been subject to long-standing discussions in the official and academic discourse. The assumption here is that higher security implies less freedom. In this regard, the Home Office responded to the Newton Report as follows: 'There is nothing new about the dilemma of how best to ensure the security of a society, while protecting the individual rights of its citizens. Democratic governments have always had to strike a balance between the powers of the state and the rights of individuals.'935

A fine balance needs to be struck to avoid abuses of the powers granted to the executive to protect civil liberties.936 In this respect, Lord Lloyd set out the “balance principle” for judging legislation in his review in 1996: ‘Additional statutory offences and

---

933 The details could be found in section 7.7.3.
934 Home Office, CONTEST: The United Kingdom’s Strategy for Countering Terrorism (Cm 8123, 2011).
935 CL Rossiter, Constitutional Dictatorship (Harcourt 1948); AS Mathews, Freedom, State Security and the Rule of law (Sweet & Maxwell 1988).
powers may be justified, but only if they are necessary to meet the anticipated threat. They must then strike the right balance between the needs of security and the rights and liberties of the individual." 937 In terms of human rights protection, the Joint Committee on Human Rights (JCHR) asserted that ‘the protection of human rights is a key principle underpinning all the Government’s counter-terrorism work,’938and in the International Commission of Jurists (2009) Report, the then Labour UK government was urged to ‘ensure that respect for human rights and the rule of law is integrated into every aspect of counter-terrorism work.’939

Similar to China, E&W attempts to find a balance between national security and human rights protection. The Home Office has stated that ‘the first priority of any government is to ensure the security and safety of the nation and all members of the public.’940 It could however be argued that preventive terrorism-related offences in E&W have favoured one aspect over the other – usually national security over human rights.

Mill claimed that the fulfilment of the state’s preventive role may be potentially dangerous to individual rights.941 Therefore, Mill considered what restrictions should be imposed when the state exercises preventive powers. Here, a crucial question raised by Mill was ‘how far liberty may legitimately be invaded for the prevention of crime.’942 Thus, preventive terrorism-related offences should be constrained by the basic principles of criminal law.

For the purpose of prevention, E&W has already enacted legislation to criminalise a wide range of offences to allow early intervention, which may lead to the conviction of innocent people. For instance, under s 58 of TA 2000, the offence may be extended to
capture acts of possession of material likely to be used to commit an act of terrorism without the need for any terrorism intention. The result of this is that people are required to ‘forego options that are themselves valuable,' thus impacting on their liberty. Although enacting preventive terrorism-related offences is done to increase public safety, the establishment of these offences could potentially negatively affect the rights of individuals or certain groups due to unwarranted coercion by the State.

There are doubts as to whether these preventive offences are effective in achieving their prevention goals though. For example, although these extensions of criminal law apparently run the risk of overreaching and unjust law enforcement, the actual number of persons convicted under these offences has been very small since 2001. This implies the measures are ineffective in preventing terrorism, perhaps serving a deterrent effect. The consensus among scholars is that there is no clear evidence that counter-terrorism measures are effective in preventing terrorism, and that in some cases the adoption of harsher laws and penalties may be counter-productive. For example, broad definitions of terrorism and executive measures potentially capture a wide range of political activities, so the risk of civil rights erosion by these measures may be greater than that of terrorism.

Although the objective of the UK government's enactment of legislation is to prevent acts of terrorism on the one hand, it must be effective and protect the rights and freedoms of individuals and maintain adherence to the rule of law. For example, the

---

943 TA 2000, S 58.
946 In the period from Sep 2001 to 31 Mar 2015, 2944 people have been arrested for terrorism-related offences. Of these, a total of 744 people have been charged with terrorism-related offences, with 449 of them being charged with offences under counter-terrorism acts. However, only 223 people have been convicted of terrorism related offences under the counter-terrorism acts. Home Office, Operation of police powers under the Terrorism Act 2000 and subsequent legislation: Arrests, outcomes, and stop and search, Great Britain, financial year ending 31 March 2015 (Statistical Bulletin 04/15, Sep 2015), data table A 03.
Home Secretary should first grant wide powers, which are then subject to independent judicial review and reviewable by the Independent Investigatory Powers Commissioner.949 However, allowing for the extension of inchoate liability to achieve further prevention goals may negatively affect individual rights, the rule of law, and basic principles of criminal law.950 Criminalisation of terrorism-related offences should respect the fundamental human rights and basic principles to ensure that the reach of criminal law is not extended unjustifiably in the name of prevention.

Similar to China, although E&W tends to give priority to national security in anti-terrorism policy and substantive laws, it can be said that there is a certain degree of balance between collective security and individual rights protection through closer examination of E&W's preemptive measures in judicial practice. In other words, there is a huge difference in anti-terrorism practices, driven by the role and importance of judicial review, judicial independence, and the over-arching scrutiny provided by commissioners and parliamentary committees.

7.4 Vague and Overbroad Definition of Terrorism

Similar to China, there is no specific definition of cyberterrorism in E&W's anti-terrorism legislation, with the existing definition of terrorism relied on instead. Therefore, as the starting point for defining cyberterrorism and terrorism-related offences, it is necessary to critically examine the scope of the definition of terrorism. Perhaps the most eye-catching innovation of the Terrorism Act 2000 (TA 2000) was the stipulation of a broad definition of terrorism for the first time,951 which covers religiously motivated international terrorism952, and proscribed organisations in a broad way. Although the


950 For further explanations of “perversions” of the criminal law as a result of their extension based on preventive goals, see RA Duff, ‘Perversions and Subversions of Criminal Law’ in RA Duff and others(eds), The Boundaries of Criminal Law (Oxford University Press 2011).

951 TA 2000, S 1: “terrorism” means the use or threat is designed to influence the government or to intimidate the public or a section of the public, and for the purpose of advancing a political, religious or ideological cause; especially mentioned “ is designed seriously to interfere with or seriously to disrupt an electronic system.” This section was amended by section 24 of the Terrorism Act 2006 and s 75 of the Counter-Terrorism Act 2008.

952 S 24 of the Terrorism Act 2006 amended sub-section(1)(b) so as to include within the definition of terrorism actions or threat of actions that are designed to influence international governmental organisations. This was inserted to remove the disparity between the original UK definition and the
term “cyberterrorism” is not explicitly mentioned in this definition, it stipulates that ‘seriously to interfere with or seriously to disrupt an electronic system’, which alludes to a form of cyberterrorism. The TA 2000 attached importance to cyberterrorism by expanding the definition to embrace terrorists’ disruptive online activities. This indicates that cyberterrorism was classified as a terrorist-related offence, with this particular behaviour viewed differently from other computer-related offences. It could be observed that cyberterrorist offences are usually prosecuted and punished under the general definitions of terrorism in the E&W and China, which means the condition of "connection with information technology" is not necessary for the act to be regarded as a special type of crime. Additionally, the distinction between cyberterrorist offences and other computer-related offences depends on the intention of the participants.

Under s 1 of TA 2000, three collective elements are required to constitute terrorism: the method, the target, and the motivation (causes). Underpinning CONTEST, this definition serves as the cornerstone for various preventive terrorism-related offences and counter-terrorism powers, so it is necessary to clearly articulate the elements of this definition in order to determine its scope and impact on preventive terrorism-related offences. The definition of terrorism has triggered fierce controversy, which has been discussed in a wealth of academic literature. Firstly, the definition of definitions of terrorism in other international instruments, for example the EU Framework Decision of 13 June 2002 on Combating Terrorism, and the International Convention for the Suppression of Acts of Terrorism. This amendment allows the definition of terrorism to apply to acts committed or threatened against international bodies such as the UN. See Explanatory Notes to TA 2006, para 158.


For example within UK law, terrorism is defined under section 1 of the Terrorism Act, 2000, with the Anti-Terrorism, Crime and Security Act, 2001 adding extra provisions, Part of the definition is harm based (subsection 2) and it is only here where anything like a concept of cyberterrorism emerges since any action is deemed to count as ‘terrorist’ if it “is designed seriously to interfere with or seriously to disrupt an electronic system” (TA 2000 sub-section (2)(e). The inadequacy of this legal conception is evident enough for it is clearly permits many actions which may have no relation to terrorism (such as a hacktivist style trespass) to be treated as terrorist acts.


terrorism has been criticised mainly for being overbroad and thus violating the principle of legality. For example, the “method” element of the definition is broad, and not only includes serious violence but also includes the threat of violence. The harm threshold is quite low and extensive, covering death and serious bodily harm as well as serious damage to property, and serious interference with or disruption of an electronic system. It seems unlikely that the damage to property or electronic systems caused what was considered a necessary companion for terrorist violence. Furthermore, there are doubts as to whether such relatively lesser harms are worthy of intervention.

Hardy and Williams held that the principle of legality is employed as the normative framework when drafting and assessing definitions of terrorism. Likewise, it could...
be argued that the definition of terrorism under s 1 is ‘immensely broad and imprecise’ and furnishes a basis for laws that are uncertain, overly expansive, and unpredictable. The breadth and vagueness of the definition of terrorism is all the more problematic because it allows for the extension of inchoate and associative liability.

According to the report of the United Nations High Commissioner for Human Rights (UNHCHR) in 2001: ‘many States have adopted national legislation (including the UK) with vague, unclear or overbroad definitions of terrorism.’ Meanwhile, the Eminent Jurists Panel of the International Commission of Jurists responded similarly, stating that some countries (including the UK) have enacted vague and overbroad definitions of terrorism or terrorist acts in their domestic law.

The broad breadth of definition of ‘terrorism’ and ‘terrorist-related activity’ may permit overbroad discretion to confer control orders under Prevention Terrorism Act (PTA) 2005, which violates the principle of certainty. For example, in the case of Secretary of State for the Home Department v E, the defendant argued that the control order granting broad powers based on a broad definition of terrorism violated the principle of certainty, which infringed the principle of “legal certainty” required by Article 5, 10 and 11 of the ECHR. The Administrative Division of the High Court insisted that it intends to interfere with the fundamental rights and freedoms of their citizens. That presumption can be displaced if a government specifies in legislation that a particular type of conduct will attract criminal punishment. In order for that criminal legislation to be valid and legitimate, it must specify a crime in advance by using language that is sufficiently clear, precise, and narrowly focused on the prohibited conduct such that individuals can reasonably foresee whether their actions will attract criminal punishment. K Hardy and G Williams, ‘What is “Terrorism”?: Assessing Legal Definitions’ (2011) 16 UCLAJILFA 77.


He explained that: ‘these ambiguous definitions have led to inappropriate restrictions on the legitimate exercise of fundamental liberties, such as association, expression and peaceful political and social opposition. UN the Office of the Higher Commissioner of Human Rights(UNOCHR), ‘Report on the protection of human rights and fundamental freedoms while countering terrorism’, UN Doc (A/HRC/8/13), paras 20-23.


E was a Tunisian national who had claimed asylum on his arrival in the UK in 1994. He was detained in 1998 after having been convicted in absentia by a Tunisian military court of putting himself at the
did not violate the principle of legal certainty because it is common for statutes and common law principles to be framed in broad terms and such breadth is not in itself a cause of uncertainty.969

Lord Carlile, a former Independent Reviewer of Terrorism Legislation, held that the definition in s 1 of TA 2000 was not ‘too wide to satisfy the clarity required for the criminal law’.970 He admitted that the definition may be extended inappropriately to apply to those who are not terrorists.971 Furthermore, he held that relying on police and prosecutorial discretion to ensure appropriate application of the definition could resolve any issues regarding its breadth and uncertainty.972 Anderson, however, believes that excessive reliance on discretion may undermine the rule of law and lead citizen to become unclear as to whether their actions will be considered innocent or criminal.973 The same sentiment was expressed by Lord Bingham in the 2001 decision of R v K, where he stated: ‘The rule of law is not well served if a crime is defined in terms wide enough to cover conduct which is not regarded as criminal and it is then left to the prosecuting authorities to exercise a blanket discretion not to prosecute to avoid injustice.’974

The intended purpose of the TA 2000 is to deter, prevent and investigate “heinous crime” in the form of acts of terrorism, which are directed toward destroying ‘not only lives, but the foundation of our society.’975 One way to assess whether a definition is too broad is to assess whether the definition exceeds its intended purpose.976 However, after assessing the definition of terrorism, it appears that it applies to an overly broad and uncertain category of conduct, which exceeds the intended purpose.

disposal of a terrorist organization operating abroad, but was released after 3 days. In 2002 he was certified under the Anti-Terrorism Crime and Security Act 2001 and detained in Belmarsh prison. In 2005, he was one of ten detainee who were subjected to a control order under the Prevention of Terrorism Act 2005.

969 Ibid, para 186.
970 Lord Carlile, The Definition of Terrorism (Cm 7052, 2007) para 26.
971 Ibid, para 60.
972 Ibid, 60-64.
975 HC Deb 14 December 1999, vol 341, col 156.
976 Hardy and Williams suggest three criteria for assessing definitions of terrorism: (1) ‘a legal definition of terrorism should be sufficiently clear and precise to give reasonable notice of the kinds of conduct it prohibits’; (2) ‘a legal definition of terrorism should not encompass conduct which allows legislation to operate outside its intended purposes’; and (3) ‘a legal definition of terrorism should be consistent with legal definitions of terrorism in comparable jurisdictions’. K Hardy and G Williams, ‘What is “Terrorism”? Assessing Domestic Legal Definitions’ (2011) 16 UCLAJLFA 77, 104, 105, 107.
For example, political protest could fall within the scope of the definition of terrorism. In such circumstances, the anti-terrorism legislation could be applied improperly to target political protests and actions which should rather fall under the purview of public order offences or regulations.

Secondly, certain phrases and terms in this definition are vague, which might lead to arbitrary judicial application. These undefined phrases and terms have resulted in rather low thresholds, violating the principle of certainty. For instance, the target requirement is that acts should ‘influence the government or an international organization’ or intimidate the public or a section of the public. Lord Carlile QC said that the target element in the definition sets a remarkably low bar when it comes to the word "influence." Anderson also criticised the wording of the definition of “influence” for setting a relatively low threshold compared to other jurisdictions (such as the EU and the US), which adopt terms such as “unduly compel,” “influence by intimidation,” “coerce, intimidate” and “force.” The wording of the definition of “influence” is so broad that it could potentially capture any political activities such as the strike action by junior doctors in 2016. Therefore, it is arguable that it is broad and not stringent use the word “influence”. In addition, civil disobedience such as violent actions by student protesters in the winter of 2010 could also fall under the

---

979 Legal terms must be clear and precise, analysis drawn from Lord Carlile of Berriew Q.C, The Definition of Terrorism (Cm 7052 2007) 21.
980 International organisation was added to section 1 of the Terrorism Act 2000 by an amendment brought in by the Terrorism Act 2006, s 34(a)
981 Terrorism Act 2000, s 1 (1)(b).
982 Lord Carlile of Berriew Q.C, The Definition of Terrorism (Cm 7052 2007) para 59.
984 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, s 2331, Part 1 Chapter 113B (ii) of the US Code 18. However, when assessing domestic terrorism the threshold is lowered to ‘influence the policy of a government’, under Part 5B(ii).
definition of terrorism because it “influenced" the UK government.988

Although the security departments and the executive recognise the preventive function of this definition, it has been criticised for being overly broad and leaving some terms undefined.989 Thus, it could be argued that the definition of terrorism should avoid ambiguous phrasing to the maximum extent possible.

Thirdly, the proliferation of the “motivation” element may broaden the definition of terrorism, encapsulating a broad range of behaviours.990 There is substantial debate among scholars as to whether the motivation element is needed in the definition of terrorism. 991 Saul and Walter held that the motivation requirement is key to distinguishing terrorism offences from other ordinary crimes.992 On the contrary, Roach argued that the motivation element is not necessary.993 Elsewhere, Anderson eventually suggested that the motivation requirement should not be abolished, as he argued that it would render the definition of terrorism even broader.994 Moreover, he suggested that the motivation element should be ‘trimmed’ to render the definition clearer and more precise.995 Walker expressed a similar view that E&W’s definition of

989 Lord Carlile, The Definition of Terrorism (Cm 7052, 2007) 22.
990 S 27 of the Counter-Terrorism Act 2008 amended sub-section(1)(c) to include acts committed for a racial cause. This is consistent with the recommendation by Lord Carlile in his 2007 report on the Definition of Terrorism, which should be amended to “ensure that it is clear from the statutory language that terrorism motivated by a racial or ethnic cause is included”. Lord Carlile, The Definition of Terrorism (Cm 7052, 2007) 48, recommendation 12. While racial causes would often fall within political or ideological causes, this amendment was intended to ‘put the matter beyond doubt that such a cause is included’. Explanatory notes to Terrorism Act 2008, para 203.
991 For opposing views on the motive element see Saul, “The Curious Element of Motive in Definitions of Terrorism: Essential Ingredient or Criminalizing Thought?” and K Roach, ‘The Case for Defining Terrorism with Restraint and without Reference to Political or Religious Motive’ in A Lynch, E MacDonald and G Williams (eds), Law and Liberty in the War on Terror (The Federation Press 2007)
terrorism is overbroad and should focus on the political motivation behind terrorist action. Although the rule of law requires legal clarity, the UK government has not given a precise definition of the motivation element, which results in a certain degree of flexibility in enforcement and court interpretation when the law is applied.

There are many questions related to the differences between religious and political, as well as racial and ideological causes. Anderson did not consider it necessary to distinguish between different kinds of motivations, but summarised religion, ideology, and ethnic motivations as political motivation. Meanwhile, Schmid claimed that it is difficult for the courts to assess whether terrorist activities are motivated by political or religious reasons.

Although adding religious motivation was largely to deal with the increasing threat of Islamic terrorism, this may have a negative impact on Islamic countries, and damaging Islamic communities and relations with them, which may contravene the principle of non-discrimination. For instance, the early preventive strategies under the UK’s CONTEST policy proved to be divisive, and the religious element in this definition may even have resulted in Islamophobia. In addition, the phrase “ideological cause” in this definition could be interpreted as a ‘catch-all’ cause. The broadness of the term “ideological” might capture any dissenting activities such as those of animal rights groups or anti-abortion groups.


Fourthly, the broad and vague definition of terrorism may also render the scope of specific terrorism offences very wide and permit broad discretion with regard to the designation of terrorists. The enactment of excessively wide definitions of terrorism has raised a core human rights problem which is central to the rule of law, namely violations of the principles of certainty and legality. The prevention of terrorism may in fact have the opposite effect. The wide-reaching definition serves to further extend the reach of the criminal law through the establishment of preventive offences to criminalise acts of innocence or remote harm, which may violate the principle of minimal criminalisation.

7.5 Criminalisation A Wide Range of Terrorism Precursor Offences

Walker argued that the first function of criminal law is to allow for prescient intervention against terrorism risks and well before a terrorist crime is committed. Today, terrorists use the Internet to support their political or military interests, such as internal and external communications, fund-raising, recruitment, training and propaganda. Like China (see Chapter 5), E&W has criminalised a wide range of precursor offences, such as the following acts which could also potentially be committed on the Internet:

- Support for a proscribed organisation (TA 2000, s 12)
- Fund-raising for terrorist purposes (TA 2000, s 15)
- Use or possession of money or other property for terrorist purposes (TA 2000, s 16)
- Possession of an article for terrorist purposes (TA 2000, s 57)
- Collecting information or possessing a document likely to be useful to a terrorist (TA2000, s 58)
- Inciting terrorism overseas (TA 2000, s 59)
- Encouragement of terrorism (TA 2006, s 1)
- Dissemination of terrorist publications (TA 2006, s 2)

---

The standard of liability associated with these offences is lowered (e.g. the requirement for **mens rea** is recklessness rather than intention, or otherwise through forms of absolute or strict liability). The rationale underpinning such an extension of criminal liability is based on risk mitigation, which also shifts the emphasis of criminal law toward precautionary prevention of crime. Such offences are designed to capture early forms of criminal conduct which are thought to causally contribute to a potential terrorist attack. The underlying rationale here is that due to the clandestine nature of terrorism and its potentially catastrophic damage, authorities should intervene at an early stage before an actual terrorist attack is committed. The criminal law has never been purely reactive and has always performed a preventive function of some sort, allowing early intervention in and prosecution of criminal conspiracies or attempts for instance. However, the earlier the criminal law intervenes, the higher the risk of capturing conduct which is remote from any actual or imminent terrorist harm. One advantage of applying inchoate offences is that it may prevent the escalation of terrorist campaigns though. However, the establishment of such offences may result in the violation of the principle of legality due to overbroad application.

Therefore, as the main mechanism to respond to these threats, the criminal law is utilised to prevent or avert the anticipatory risk of terrorism. Conversely, traditional criminal law generally intervenes after, rather than before, a criminal event and in

---

judicial practice there are also some obstacles to early intervention regarding to admissibility, disclosure and proof.\textsuperscript{1013} Terrorism precursor offences significantly expand the boundaries of the criminal law.\textsuperscript{1014} They not only apply to acts that are remote from real harm than the inchoate offences, but also punish a wider range of participants (including those who have not directly committed terrorist acts but have an associative or facilitative role).\textsuperscript{1015} According to Anderson, the Independent Reviewer of Terrorism Legislation, the expanded reach of criminal law and early intervention may loom over previously innocent interactions.\textsuperscript{1016}

7.5.1 Criminalisation of Membership of Terrorist Organisations Online and Offline

One of the most prominent extended anti-terrorism offences to have been established is membership of a terrorist organisation, as well as related offences of association with members and/or the organisation.\textsuperscript{1017} Rationales behind association offences are crime prevention and protecting the public from the dangers of terrorism and enhancing security. For example, the UK government stated that ‘the purpose of the proscription offences was threefold: to deter, to target low-level support, and to signal condemnation.’\textsuperscript{1018} Furthermore, the aim of prohibiting even innocent or harmless support or participatory acts is to prevent the future potential risk of harm on the part of terrorist organisations.\textsuperscript{1019} In addition, Walker argued that ‘proscription has often

\begin{footnotesize}
\begin{itemize}
\item\textsuperscript{1014} S Macdonald, ‘Prosecuting Suspected Terrorists: Precursor Crimes, Intercept Evidence and the Priority of Security’ in L Jarvis and M Lister(eds), \textit{Critical Perspectives on Counter-terrorism} (Routledge 2014).
\item\textsuperscript{1017} See, e.g, EU Framework Decision on Combating Terrorism of 2002, art. 2(2), which requires States to punish to contribute to the any way, with knowledge of the fact that such participation will contribute to the criminal activities of the terrorist group’. See also TA 2000 (UK), which establishes various offences relating to a proscribed organization: belonging or professing to belong to it (s. 11(1)), inviting support for it (s. 12(1)), arranging, managing, or assisting in arranging or managing, a meeting of it (s. 12(2)), advertising a meeting to encourage support for or further the activities of it (s. 12(3)), and appearing in public displaying allegiance with or support for it (s. 13(1)); directing an organization is also an offence, which does not require proscription (s. 56).
\item\textsuperscript{1018} Standing Committee D, col 56 (HC, 18 Jan 2000), Charles Clarke.
\item\textsuperscript{1019} D Cole, ‘Terror Financing, Guilt by Association and the Paradigm of Prevention in the ‘War on
\end{itemize}
\end{footnotesize}
been of marginal utility in combating political violence.' He held that these offences are only symbolic because the number of convictions for proscription offences is low.

However, the identification of a person’s membership of or association with a terrorist organisation offences raises some issues. Firstly, as the UN Special Rapporteur has observed, there is a need for ‘precision and clarity’ in the definition of the link between a terrorist organisation and the individual’s actions, since expressions such as ‘support,’ ‘involved in’ or ‘associated with’ inevitably ‘leave much leeway for interpretation, uncertainty of liability for individuals, and improper criminalization.’

S 11(1) of TA 2000 sets out that ‘a person commits an offence if he belongs or professes to belong to a proscribed organization.’ Indeed, the meaning of the word ‘profess’ is somewhat uncertain. Apart from the vagueness of the language in s 11(1), the actus reus of proscription offences are also overly broad. Accordingly, it could be argued that these offences may violate the principle of certainty.

Secondly, under s 11(1) of TA 2000, there is no mens rea requirement, which implies that such offences are of strict liability. The lack of an actus reus requirement or any mens rea requirement means that acts without any terrorism intention may be covered. S 11(2) places a reverse burden of proof on the accused. However, it can be hard for the accused to exercise their right of defence effectively, which may result in potentially severe consequences (the maximum sentence is 10 years’ imprisonment).
The membership offences reflect the criminalisation of a very remote risk of harm, with no requirement of a future harmful act of terrorism being planned or even contemplated. In addition, this offence extends liability laterally by criminalising a wide range of assorted facilitative, associative or participatory acts, which may violate the principle of minimal criminalisation.

7.5.2 Criminalisation of Propaganda, Incitement and Dissemination of Terrorism

Terrorists have increasingly used the Internet for propaganda, incitement and dissemination, and social media as a convenient channel has long been exploited by terrorists to disseminate their ideology and to pursue their political ends. According to Imran, s 1 and s 2 of TA 2006 enables law enforcement bodies to further expand the scope of suspicion, enabling ever more ‘expansive possibilities for the prosecution and conviction.’ Theses sections were aimed at criminalising ‘speeches at meetings, broadcasts and material posted on the Internet.’

S 1 of TA 2006, which criminalises direct or indirect encouragement (including glorification) of terrorism, has been controversial as the punishment for this offence is up to seven years’ imprisonment. The other main precursor offence is concerned with the dissemination of terrorist publications. This provision stipulates various of means of disseminating terrorist publications, including ‘the transmission of the publication electronically.’ Unlike S 1 of TA 2006, which is the response to originators of statement, s 2(1) of TA 2006 deals with the secondary dissemination of

---

1027 C Walker and M Conway, ‘Online Terrorism and Online Laws’ (2015) 8(2) DAC156, 156.
1028 Robert Bowers, the suspect perpetrator of the 10.27 Pittsburgh synagogue shooting created on his account on Gab, and posted before the massacre that: “HIAS, a Jewish non-profit organization, likes to bring invaders in that kill our people. I can’t sit by and watch my people get slaughtered. Screw your optics, I’m going in.” The shooter was reported to post extreme, hateful and anti-Semitic contents on Gab, even shouting “all Jews must die” before opening fire. Social media once again was debated and criticized because of the unlimited tolerance for such speeches, though Gab made a statement after this shooting that “Gab unequivocally disavows and condemns all acts of terrorism and violence.”
1031 Other new offences regard the dissemination of terrorist publication (s.2), the preparation of terrorist acts (s.5) (the maximum penalty in this case is life imprisonment), and training for terrorism (s.6), to name a few.
1032 Terrorism Act 2006, s 2.
1033 TA 2006, s 2(2). The means of dissemination: distribution or circulation; giving, selling or lending; offering it for sale or loan; providing a service enabling others to obtain, read, listen to or look at it or acquire it by means of a gift or loan and electronic publication.
terrorist publications with intent or reckless as to direct or indirect encouragement to acts of terrorism.\textsuperscript{1034} The Third Report of the Joint Committee on Human Rights raised human rights concerns about this particular clause, and suggested inserting defences of reasonable excuses or public interest to rule out criminalisation, thereby protecting legitimate activities of the media and academics.\textsuperscript{1035}

The rationale underpinning these two sections respond to Article 5 of the Council of Europe’s Convention on the Prevention of Terrorism (CECPT), which requires state parties to criminalise ‘public provocation to commit a terrorist offence.’\textsuperscript{1036} However, this response has caused some problems.

(1) The \textit{actus reus}\textsuperscript{1037} is clearly very broad, thus widening its application.\textsuperscript{1038} Under this provision, the perpetrator should publish a statement, which could be a formal statement (s 20(6)) or published in any means (s20(4)) (e.g. through an electronic service).\textsuperscript{1039} It also includes using a service provided ‘electronically by another so as to enable or to facilitate access by the public to the statement.’\textsuperscript{1040} So, for example, a statement posted on a website run by someone else (such as a website owner or Internet service provider) could be punishable under this offence.\textsuperscript{1041}

In addition, this offence criminalises both direct and indirect encouragement, with the definition of the latter criticised for being too nebulous and broad. The reason behind criminalising indirect encouragement is that these acts could ‘create the climate of hate

\textsuperscript{1034} Terrorism Act 2006, s 2(1).
\textsuperscript{1036} Art. 5 of CECPT. HL Deb 5 Dec 2005, vol 676, col 435.
\textsuperscript{1037} Terrorism Act 2006, s1(2)(a).
\textsuperscript{1039} Terrorism Act 2006, s 20 (5): providing a service includes making a facility available.
\textsuperscript{1040} A Hunt, ‘Criminal Prohibitions on Direct and Indirect Encouragement of Terrorism’ (2007) CLR 441, 444. It is interesting to note Al Shabaab and other terrorist organisations have Twitter accounts from which they tweet updates, many of which could be caught under this offence, see John Hudson, ‘The Most Infamous Terrorists on Twitter’ (\textit{The Atlanticwire}, 2 January 2012) \texttt{<http://www.theatlanticwire.com/global/2012/01/most-infamous-terrorists-twitter/46852/>} accessed 20 Jan 2020.
in which terrorism can more easily flourish.\footnote{Hazel Blears MP, HC Deb 9 November 2005, vol 439, col 430.} However, as Roach rightly points out, Lord Carlile’s conclusion was ‘flawed in its assumption that the criminalization of speech is rationally preventing terrorism.’\footnote{See K Roach, ‘A Comparison of South African and Canadian Anti-Terrorism Legislation’ (2005) 18(2) SAJCJ127, 127-150; K Roach, ‘The Case for Defining Terrorism with Restraint and without Reference to Political or Religious Motive’ in A Lynch, E Macdonald and G Williams (ed), \textit{Law and Liberty in War on Terror} (The Federation Press 2007) 39-49.}

E&W does not define the term “indirect encouragement,” the boundaries of which are hard to clarify. Furthermore, the line between direct and indirect encouragement is difficult to distinguish.\footnote{S Macdonald, ‘Social Media, Terrorism Content Prohibitions and the rule of law’ (2019) PEGWU 1,7.} Whether indirect encouragement (such as praise, glorification of terrorism, defending terrorism, vilifying victims or calling for funding of terrorist organisations) should be criminalised or not has been the focus of long-standing controversy in E&W.\footnote{A Jones QC, R Bowers and HD Lodge, \textit{Blackstone’s Guide to The Terrorism Act 2006}, (Oxford University Press 2006) 13.} Sometimes, indirect encouragement is more compelling than direct encouragement.\footnote{J Searle, ‘Indirect Speech Acts’ in P Cole and JL Morgan (ed), \textit{Syntax and Semantics, Volume 3: Speech Acts} (Academic Press 1975).} It is also important that the boundaries of prohibitions on terrorism-promoting content are communicated as clearly as possible.\footnote{S Macdonald, S Correia and A Watkin, ‘Regulating Terrorist Content on Social Media: Automation and the Rule of Law’ (2019) 15(2)JLCLC 183, 183-197.} This allows people to understand their rights and responsibilities before posting a statement to the public. Furthermore, some have questioned whether criminalisation of such offences is in compliance with the principle of minimal criminalisation.

According to s 1(3),

\begin{quote}
Glorify committing a terrorist act or prepare to commit a terrorist act (whether or not the act has occurred in the past, the future, or the present), and such speech or publication can enable those members of potential publics to reasonably infer what behavior is glorified, and be emulated by them in the real world, and this behavior is the offence of indirectly encouragement of terrorism.\footnote{Terrorism Act 2006, s 1(3)(b).}
\end{quote}
Here, glorification means ‘any form of praise or celebration,’ which has been notably criticised on the grounds of uncertainty and vagueness. It is irrelevant to the establishment of this offence whether someone is actually encouraged to commit terrorism. A working (non-legal) definition was proffered by a Home Office Minister as follows: ‘to glorify is to describe or represent as admirable, especially unjustifiably or undeservedly.’ For example, a statement containing glorification of the bombing of a bus at Tavistock Square on 7 July 2005, and inciting the public to repeat this event, may be interpreted as encouraging the public to emulate attacks on the public transport system. The UK government’s advice to those who wish to avoid glorification of terrorism is to declare before their statement that they do not condone, or support or incite the public to commit terrorist acts. They can express sympathy and even support for this activity, but they cannot encourage people to commit terrorist acts. This provision is particularly controversial: in particular, glorification can be understood as an indirect encouragement of terrorist acts, which leads to reasonable inference and emulation on the part of the public. As a result, the clause was deemed ambiguous and uncertain, and was strongly criticised by the Joint Committee of the House of Lords and the House of Commons on Human Rights. There were two specific concerns raised about the word “glorifies”: firstly, it was considered broad and vague under the explanation in s 20(2) of TA 2006 which ‘includes any form of praise or celebration’; and, secondly, the maximum penalty for this offence was deemed excessive, standing at seven years’ imprisonment.

(2) As for the mens rea, under s 1 of TA 2006, the offence of ‘encouragement of terrorism’ requires intention of recklessness. Since proof of recklessness will suffice, there is no requirement to prove a terrorist purpose. Under s 1(6), the defendant could provide a defence of non-endorsement in case of recklessness if he

---

1049 Terrorism Act 2006, s 20(2).
1051 Terrorism Act 2006, s 1(5)(b).
1054 HC Deb 9 Nov 200, vol 439, col 429. See also HL Deb 5 Dec 2005, vol 676, col 458.
1056 A Ashworth and J Horder, Principles of Criminal Law(7th edn, Oxford University 2013) 69.
1057 Terrorism Act 2006, s 1 (2)(b).
can show that ‘the statement neither expressed his views nor had his endorsement’ and that this is clear ‘in all the circumstances of the statement’s publication.’ The recklessness requirement of the offence runs counter to the general principle that inchoate offences should require the highest mens rea test because of the remoteness between the offence and the commission of the ultimate harm.

HRW criticised the ambiguity of the mens rea of this offence is unclear. Moreover, the United Nations Human Rights Committee (UNHRC) described the definition of ‘encouragement of terrorism’ in s 1 of the TA 2006 as ‘broad and vague.’ In particular, the establishment of this offence does not require intention of perpetrators, as long as their statements cause the public to commit a terrorist act. Therefore, the UNHRC recommended that the UK amend its wording to avoid ‘excessive interference with freedom of expression’ guaranteed by Article 19 of the ICCPR.

(3) Another problematic issue in this regard is related to the threshold of harm. According to s.1(1), as long as the statements or publications are likely to be understood by ‘some or all of the members of the public,’ the offence of encouragement of terrorism could be established. The establishment of the encouragement of terrorism offence does not require the actual commission of a terrorist act as a result of encouragement, nor does it require that there may be a risk of encouraging terrorist acts. This can be contrasted with the requirement in the CECPT that the conduct must cause ‘a danger that one or more such terrorist offences may be committed.’ Therefore, the offence of encouragement of terrorism in E&W

---

1058 Terrorism Act 2006, s 1(6)(a)
1063 Ibid.
1064 Terrorism Act 2006, s 1(1).
is broader than Article 5 of the CECPT, because s 1 contains no such restriction as to an objective danger of the commission of a terrorist offence as a result of encouragement.1067

(4) It has been argued that the criminalisation of indirect encouragement may infringe freedom of expression because such criminalisation is too ambiguous and discretionary, which may violate the principle of legal certainty and proportionality to cope with the threat of radicalisation.1068 For example, HRW criticises this offence for lacking clarity and certainty, making it difficult to regulate their behavior to avoid violating the provision and potentially violating citizens' freedom of speech.1069

Because the provision criminalises ‘praising terrorism,’ it makes it difficult for individuals to predict whether their speech will constitute incitement to terrorism or will be accepted as a legitimate act of freedom of expression. HRW also criticised the Terrorism Bill 2005 for not requiring a causal relationship between incitement and actual violence.1070

Article 10 of the ECHR protects the right to freedom of expression, including ‘the freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.’1071 However, this right can be limited in certain circumstances, including ‘in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime.’1072

According to Article 19(3) of the ICCPR, freedom of speech can be restricted to some extent when necessary to respect the rights or reputation of others, or to protect national security or public order.1073 Article 10 of the ECHR specifically states that any restrictions on the right to freedom of expression must be ‘prescribed by law’ and must

1067 Council of Europe Convention on the Prevention of Terrorism, art.5(2).
1068 The conflict with the freedom of speech has been addressed by many. See E Barendt, Freedom of Speech (OUP 2005); K Roach, ‘Must We Trade Rights for Security? The Choice between Smart, Harsh or Proportionate Security Strategies in Canada and Britain’(2006) 27(5)CLR 2151, 2157, 2181.
1070 Ibid.
1071 ECHR, Art 10(1).
1072 ECHR, Art 10(2).
1073 ICCPR, Art. 19(3).
be ‘necessary in a democratic society.’ Furthermore, restrictions should be narrowly interpreted and the means used must be commensurate with the purpose to be achieved. This implies that this offence must comply with the principles of certainty and proportionality. Such an offence might create tensions with respect to the proportionality principle, as a glorification offence, with its wide scope and interpretative difficulties, could be seen as excessive interference. In principle, for the purposes of crime prevention and public order protection, the prohibition of incitement to terrorism may constitute a reasonable restriction on freedom of expression. The key issue here is how to distinguish between licit and illicit speech.

The Joint Committee on Human Rights (JCHR) considered only some forms of indirect incitement to violent terrorism to be in line with Article 10 if they were necessary, proportionate and defined so as to satisfy the requirements of legal certainty. The Committee argued that the law should consider:

...that the offence of encouragement in s 1 is not sufficiently legally certain to satisfy the requirement in Article 10 that interferences with freedom of expression be “prescribed by law” because of (i) the vagueness of the glorification requirement, (ii) the breadth of the definition of “terrorism” and (iii) the lack of any requirement of intent to incite terrorism or likelihood of such offences being caused as ingredients of the offence.

The right of freedom of speech is critical in the context of counterterrorism. As Barendt stated: ‘We can only respond intelligently to undesirable extremist attitudes, and remove or reduce the reasons why they are held, if we allow them, to some extent, to be disseminated.’ One of the chief criticisms of the E&W’s encouragement of

---

1074 ECHR, Art.10(2).
1075 Sunday Times v UK (1979) 2 ENRR 245, para.65.
1080 Ibid, p.3 and paras 27-33.
terrorism offence has been that it is overly broad and, as a result, has a chilling effect on free speech. For example, the JCHR warned that ‘such theoretical possibility of committing the serious criminal offence of encouraging terrorism can only inhibit freedom of discussion and debate on topical and contentious political issues.’

Moreover, the impact of this chilling effect is unknown and difficult to measure, which possibly prevents people from publishing statements they may otherwise have published. As a result, individuals may be guilty of the offence under s 1 of TA 2006, but lack any normative involvement in future acts of terrorism.

(5) S 3 seeks to apply s1 and s 2 in the context of unlawfully terrorism-related articles or records on the Internet, thereby preventing terrorists or would-be terrorists using the Internet to disseminate materials and halting terrorist communication. The purpose of setting up this article is to deal with the proliferation of extremist websites, and to confirm that Internet communication technology can be both an attack target and a useful tool for terrorists. S 3(7) stipulates that “unlawful terrorism-related materials” constitutes direct or indirect encouragement or other inducement to terrorism Convention offences or contains information which is likely to be useful to any one or more of those persons in the commission or preparation of such acts.

S 1 and 2 are examples of the criminalisation of remote harm. The conduct itself does not cause harm, but rather the risk of future harm. Accordingly, this offence may violate the harm principle and the normative involvement principle. It is difficult to identify

---

1086 Terrorism Act 2006, s 3.
wrongfullness in offences of s 1 and 2 that are aimed at preventing the occurrence of future harm. Although inchoate offences require the highest *mens rea* standard, the encouragement offences in s 1 and 2 can be committed recklessly. So, there is a potential danger of criminalising non-wrongful conduct, which may result in over-criminalisation.

7.5.3 Criminalisation of A Broad Scope of Preparatory Terrorist Acts

Preparatory offences have been established to prioritise the prevention of terrorist attacks.\(^{1089}\) Therefore, unlike the ex-post punishment of traditional criminal law, these criminal offences could be punished before the commission of terrorist attacks.\(^{1090}\) In addition, these offences go further than traditional criminal offences by criminalising the formative stage of such acts and imposing serious penalties on preparators regardless of the clarity of their intentions.\(^{1091}\) To illustrate this issue, s 5 of the TA 2006 stipulates ‘offences of preparation of terrorism.’ The offence occurs if, with the intention of (a) committing acts of terrorism or (b) assisting another to commit such acts, a person engages in any conduct in preparation to give effect to that intention.\(^{1092}\)

The purpose of this offence is to extend the scope of the attempted liability to the early stages of preparation, which runs counter to the long-standing principle of attempted liability.\(^{1093}\) Liability is extended to merely preparatory conduct, which is remote from the commission of the substantive act of terrorism. Despite such remoteness, the maximum penalty for this offence is life imprisonment and many offenders have been handed lengthy sentences of 20 years or more.\(^{1094}\) Given the lack of proximity to the

---

1092 *Terrorism Act* 2006, s 5.
1093 The section 1 of Criminal Attempts Act 1981 requires that liability for attempts is limited to conduct “which is more than merely preparatory to the commission of the offence”.
commission of the ultimate harm and the harsh punishment, this offence may violate the principle of proportionality.\textsuperscript{1095}

(1) The \textit{actus reus} of s 5 is overly broad, containing a wide range of preparatory conduct.\textsuperscript{1096} Furthermore, there is no guidance to clarify what could fall within this section. The wide range of conduct has so far included travelling to an airport intending to go to Pakistan to join a terrorist operation (\textit{R v Qureshi})\textsuperscript{1097}, planning to place a bomb in an identified location (\textit{Usman Khan v R})\textsuperscript{1098}, and producing ricin sufficient to kill nine people (\textit{R v Davison}).\textsuperscript{1099} It could thus be argued that this offence violates the principles of certainty and minimal criminalisation.

(2) With respect to the \textit{mens rea}, the offenders must have the intention to commit or assist the acts. In addition, the person must have the further intent that the act or assistance will further terrorism.\textsuperscript{1100} According to section 5(2), it is expressly irrelevant whether the intention and preparations relate to one or more particular acts of terrorism, acts of terrorism of a particular description, or acts of terrorism generally.\textsuperscript{1101} With this in mind, the offence does not require proof of an identifiable final act or acts of terrorism, but the prosecution must prove a specific intent to commit a terrorist act or to assist another to do so.\textsuperscript{1102}

This section was designed to deal with cases in which individuals were actively planning acts of terrorism, and stopped before they completed or attempted a substantive terrorist act.\textsuperscript{1103} S 5 can be specifically applied to 'lone wolf' cases, which means the perpetrator acts alone, or the prosecution does not have sufficient evidence

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{1095} Joanna Simon, ‘Preventive Terrorism Offences: The Extension of the Ambit of Inchoate Liability in Criminal Law as a Response to the Threat of Terrorism’ (DPhil thesis, Oxford University 2015) 159.
\item \textsuperscript{1097} \textit{R v Sohail Anjum Qureshi} [2008] EWCA Crim 1054.
\item \textsuperscript{1098} \textit{Usman Khan and others v R} [2013] EWCA Crim 468.
\item \textsuperscript{1099} \textit{R v Davison} (Unreported, Newcastle Crown Court, Milford J, 14 May 2010)
\item \textsuperscript{1101} Ibid, p.130.
\item \textsuperscript{1103} Susan Hemming, ‘The practical application of counter-terrorism legislation in England and Wales: a prosecutor’s perspective’ (2010) 86(4) IA 964.
\end{itemize}
\end{footnotesize}
to prove that multiple people are conspiring or involved, or do not know the specific
details of the offence that was being planned.

The rationale behind the creation of this offence was to prevent the perpetration of an
act of terrorism. However, it is argued that the preventive offences must fall within the
bounds of the principle of proportionality, which means that public safety and individual
liberty should be suitably balanced. Due to the wide range of the \textit{actus reus} and the
remoteness from the commission of a terrorist act, this offence has the potential to
criminalise non-wrongful acts. In light of this, some argue that this offence violates the
principle of minimal criminalisation and the harm principle.

\textbf{7.5.4 Training for Terrorism via the Internet}

Other supporting cyber activities are those where terrorists provide instructions or
receives instructions or training via the Internet. According to s 54(4) of the TA 2000,
‘instructions’, ‘training’ and ‘invitations’ can be targeted to the general public or to
specific persons online and offline (such as by a pamphlet or via the Internet).\footnote{1104}
For instance, in the case of \textit{R v David Copeland}, the perpetrator obtained the bomb making
information from the Internet, although he was actually unable to assemble the
necessary ingredients.\footnote{1105} It was also stated by Kent Roach that s 54 of the TA 2000
is a good example of the expansionist tendencies of modern anti-terrorism law that
deals with ‘inchoate offences’ such as attempted conspiracy or remote connections
with actual acts of terrorism.\footnote{1106}

Meanwhile, offences around training are amplified by s 6 and s 8 of the TA 2006, which
relate to techniques other than specified weaponry.\footnote{1107} In addition to overlapping with
the s 54 of the TA 2000, s 6 of the TA 2006 is broader than the former. According to s
6 (1), an offence is established by the provision of instruction, training or knowledge
that the recipient intends to use for terrorism even if that is not the intention of the

\begin{footnotes}
\footnote{1104} Section 54(4) of TA 2000.
\footnote{1105} M Wolkind and N Sweeney, \textit{R v David Copeland} (2001) 41 MSL 185, 190.
\footnote{1106} K Roach, ‘Terrorism’ in M Dubber and T Hornle (eds), \textit{Oxford Handbook of Criminal Law} (OUP
2014) 16-17.
\footnote{1107} C Walker, \textit{Blackstone’s Guide to The Anti-Terrorism Legislation} (3rd edn, Oxford University Press
\end{footnotes}
provider. The element of intention of the recipient is important here and is designed to exempt university lectures in chemistry or military studies collections in public libraries. According to section 6 (4), the instruction or training in terrorism or Convention offences can be provided to a target audience or to the world in general (through the Internet), though for general instruction it would be difficult to prove the mens rea with respect to the intention of the recipients.

7.5.5 Preventive Statutory Measures: Criminalisation of Possession of Articles and Collecting Materials and Information for Terrorism Purposes

There are two further important precursor crimes related to possession with terrorist purposes in the Terrorism Act 2000: s 57 (possession of items relevant to terrorism) and s 58 (collecting or making a record of information related to terrorism). Although s 58 has a lower threshold for proof of intent than s 57, both are introduced for the purpose of prosecuting a would-be terrorist at an early stage, rather than waiting until the physical terrorist activities have been completed. These two sections stoked much controversy during their passage through Parliament and thereafter, most of which centred on the broad actus reus of the offence and the reverse burden of proof. These provisions are also regarded as anticipatory offences, with a correspondingly broad range that may potentially capture an excessive amount of citizens.

“Article” is further defined in s 121 of the TA 2000 to include ‘substance and any other thing,’ which is a very broad definition indeed. An article per se is usually legal and even commonplace, differing markedly from explosives, firearms, weapons, and other...
dangerous substances to which specific offences apply.\textsuperscript{1115} As Anderson pointed out, s 57 could ‘catch even such articles as cars, which are not designated for terrorism.’\textsuperscript{1116} There is no restriction on the type of article covered, as long as the article gives rise to a reasonable suspicion that its possession is for a terrorism-related purpose. In the case of \textit{R v Rowe},\textsuperscript{1117} documents and records were considered “articles” under s 57. This means that there is an overlap between s 57 and s 58, which implies that information (whether written down or stored electronically), as well as tangible articles, can fall within the ambit of s 57.

As for the \textit{mens rea}, it requires that the perpetrator has the knowledge of possession, and control over the article.\textsuperscript{1118} However, under s 57(3), the possession could be presumed in certain circumstances which are broad and easily satisfied.\textsuperscript{1119} In the case of \textit{R v G; R v J},\textsuperscript{1120} the House of Lords explained that the prosecution does not need to prove that the accused has a purpose connected with terrorism.\textsuperscript{1121}

According to s 57(2), the defendant bears the burden of proof that the possession of the given article was not for a purpose connected with terrorism. There have been many disputes as to whether the burden of proof being placed on the defendant violates the presumption of innocence.\textsuperscript{1122} It could be debated that the reversal of the

\textsuperscript{1115} See Explosive Substances Act 1883, s 4; Firearms Act 1968, s 16-21; C Walker, \textit{Blackstone’s guide to the anti-terrorism legislation} (2\textsuperscript{nd} edn, Oxford University Press 2009), 187.


\textsuperscript{1117} \textit{R v Rowe} [2007] EWCA Crim 635; [2007] 2 Cr. App. R. 14 (p 171); [2007] Q.B.975. Rowe was convicted under s 57 for the possession of a notebook containing handwritten instructions for assembling and operating a mortar, and a substitution code listing components of explosives and various places that were susceptible to terrorist bombing.

\textsuperscript{1118} \textit{R v G and J}(2009) UKHL 13, para 53.

\textsuperscript{1119} According to s 57(3), if the prosecution proves that an article was either “on any premises at the same time as the accused ” or “was on premises of which the accused was occupier or which he habitually used otherwise than as a member of the public ”, the court can presume that the defendant was in possession of the article, thus negating the implied \textit{mens rea} of knowledge and control.

\textsuperscript{1120} \textit{R v G and J}(2009) UKHL 13.

\textsuperscript{1121} Ibid, para 54, 55.

burden could adversely affect the presumption of innocence.\textsuperscript{1123}

Since the offence has a broad \textit{actus reus} and no requirements for \textit{mens rea}, it is easy to satisfy the elements of this offence for the prosecution. In light of this, it is arguable that these offences may violate the principle of minimal criminalisation.

In recent years, this offence has been used to successfully prosecute several individuals who have been found in possession of items as diverse as hard drives, DVDs and instructional documents on how to make or operate items such as mortars, suicide vests and napalm.\textsuperscript{1124} The court held that the prosecution should prove the connection between the ‘article in possession’ and the purposes of ‘commission, preparation, or instigation of the prospective acts of terrorism,’ in the case of \textit{R v Zafar}.\textsuperscript{1125} The court concluded that in order to be consistent with the principle of legal certainty, a direct connection is required between the possession and the act of terrorism.\textsuperscript{1126} Therefore, the court seemed to acknowledge that the offence targets possession that is remote from the commission of harm. Therefore, the court not only focused on narrowing the scope of conduct, but also ensuring legal certainty.

\textbf{7.5.6 Collection of Information via the Internet}

One type of ancillary cyber activity is where terrorists use the Internet to conduct intelligence-gathering or data-mining, the outcome of which could be the use of these information or data to commit terrorist attacks against the public. There are two variants of \textit{actus reus} in s 58(1): collecting or making a record of information likely to be useful to terrorism; or possessing a document or record containing information of that kind.\textsuperscript{1127} A “record” here includes photographic or electronic formats as well as writings and drawings (s 58(2)), but unrecorded mental knowledge is not covered.\textsuperscript{1128}

\textsuperscript{1123} Ibid, p227.
\textsuperscript{1126} \textit{R v Zafar} [2008] EWCA Crim 184.para 29.
\textsuperscript{1127} TA2000, S 58.
\textsuperscript{1128} C Walker, ‘Cyber-terrorism: Legal principle and the law in the United Kingdom’ (2006) 110 PSLR
The failure to specify clearly and accurately the parameters of what information is included makes the *actus reus* extremely broad. Some have argued that almost anything could be used to commit a terrorist act such as the A-Z map of London,\(^\text{1129}\) flight schedules or train timetables, legal books and articles on counter-terrorism. In the case of *R v K*, it was argued that s 58 did not fully comply with the principle of legality or the requirements of Article 7 of the ECHR.\(^\text{1130}\)

As for the *mens rea*, unlike s 57(3), the s 58 does not contain a presumption that the possession is related to terrorist acts under certain circumstances. Therefore, the defendant is required to have both knowledge and control over the record that is collected or possessed.\(^\text{1131}\) S 58 does not require proof that the defendant had a terrorist purpose or ulterior intention. Therefore, persons without any terrorist purpose or connection may be convicted of this offence. It is therefore arguable that such offences may violate the principle of minimal criminalisation.

In the case of *R v K*, the court stated that the nature of information must raise a reasonable suspicion.\(^\text{1132}\) In *R v G*, *R v J*, the court speculated that Parliament must have ‘proceeded on the view that, in fighting something as dangerous and insidious as acts of terrorism, the law was justified in intervening to prevent these steps being taken, even if events were at an early stage or if the defendant’s actual intention could not be established.’\(^\text{1133}\) As for standard of proof, the Crown must prove beyond reasonable doubt that the defendant is aware of the possession of a document or record and the nature of contents must be useful to commit, prepare, or perform other acts related to terrorism.\(^\text{1134}\) As for the burden of proof, the main controversial aspect of s 58 is that it places upon the accused a burden of proof, and according to s 58(3) the defendant has to have a reasonable excuse for his action or possession.\(^\text{1135}\)

---


\(^{1130}\) *R v K* [2008] EWCA Crim 185, para 4.

\(^{1131}\) TA2000, S 58.

\(^{1132}\) *R v K* [2008] EWCA Crim 185.


\(^{1134}\) TA2000, S 58.

\(^{1135}\) Ibid.
The scope of the term “article” in s 58 has caused huge controversy. In *R v. K*, the Court of Appeal adopted a restrictive interpretation, applying s 58 only if the document or record is likely to provide practical assistance to a person committing or preparing to commit an act of terrorism. Accordingly, the possession of theological or propagandist material is excluded from criminalisation, thereby effectively curtailing the scope of s 58.

A year later, in the case of *R v G and J*, the court reaffirmed the ‘practical use test,’ which means the person in possession of the document or record should be prosecuted only if the document would be of practical assistance in committing or preparing terrorist acts and holds no reasonable excuse for possession. It was argued that the term ‘likely to be useful’ is so broad that it may violate the principle of legal certainty, and effectively criminalises the possession of innumerable items of information. For instance, the A-Z map of London is of practical use for a whole range of things, which may therefore be considered ‘likely to be useful’ for terrorist activities. The Court of Appeal sought to remedy any imprecision and excessive breadth of the *actus reus* in the offence, to limit the type of information, so as to render it compatible with the doctrine of legality. The defendant, J, argued without success in the ECtHR that this judgment infringed the rights enshrined in Articles 7 and 10 of the ECHR. Ackerman claimed that this judgment reflected E&W’s counter-terrorism legislation being overbroad which is restricted by the judiciary, potentially causing executive excess. Therefore, some scholars have expressed that the real threat to the public does not come from terrorism, but from these overly broad anti-terrorism measures.

These offences in s 57 and s 58 of the TA 2000 are broad and indeterminate which

---

1137 *R v K* [2008] EWCA Crim 185, [13].
1140 Ibid, para 6.
1141 Ibid, para 16.
may impact upon a wide range of people such as journalists\textsuperscript{1145} and scholars\textsuperscript{1146} who study terrorism. The public, including academic scholars, access to Internet sources such as the website directory 192.com or by using documents freely available on the web, such as \textit{The Terrorist's Handbook} and \textit{The Big Book of Mischief}.\textsuperscript{1147} Under s 58, there is no need to prove that the information was obtained or held in violation of the law. A defence of 'reasonable excuse' could be used to absolve academics, journalists or others who may have a legitimate reason to view such material.\textsuperscript{1148}

This offence may cover a wide range of materials and behaviours, but the nature of the prevention of terrorism is somewhat abstract. A person’s downloading of terrorism-related materials from the Internet is more likely to be caused by curiosity than planning or preparing to commit terrorism. Nevertheless, sections 57 and 58 extend the reach of the criminal law to a point where, often based on equivocal evidence, the prospect of harm is uncertain.\textsuperscript{1149}

Sections 57 and s 58 are vaguely worded, and there is a certain degree of overlap, but there are still some important differences between the two.\textsuperscript{1150} First, s 57 applies to possession, while s 58 applies not only to possession but also to collecting or making. Secondly, s 57 covers ‘articles’ whereas s 58 covers only ‘documents or records’ which are a subset of articles. Thirdly, s 57 applies where the circumstances give rise to a reasonable suspicion of terrorist purpose, whereas s 58 focuses on the nature of the information without regard to the circumstances or purpose.\textsuperscript{1151} The overlap between the two may cause juries to be confused and even lead to the two being applied together.

\textsuperscript{1146} Scholars who study terrorism might also skirt s 58, such as Rizwaan Sabir, a postgraduate student at Nottingham University who was detained for seven days and later compensated, Sam Jones, ‘Student in al-Qaida raid paid £20,000 by police’ (The Guardian, 15 Sep 2011) <https://www.theguardian.com/uk/2011/sep/14/police-pay-student-damages-al-qaida> accessed 30 Oct 2020.
\textsuperscript{1150} See further \textit{R v G and J} (2009) UKHL 13, paras 57-9.
\textsuperscript{1151} \textit{R v Samina Malik} (2008) EWCA Crim 1450, para 43.
The court has adopted various interpretations to narrow down the application of offences, such as requiring a direct connection between the article possessed and the act of terrorism under s 57, and requiring that the article be of inherently practical utility to a terrorist under s 58. However, such interpretations have not succeeded in making these provisions sufficiently precise or narrow. Through assessing and analysing the scope and effect of sections 57 and 58, the vagueness and uncertainty of these sections has been highlighted, especially the unclear and expansive actus reus and the lack of a true culpability requirement.

Foregoing these requirements may violate the principle of sufficient normative involvement set out by Simester and von Hirsch. Information that is intrinsically useful to a terrorist and is not easily acquired could be considered for future use. However, such normative involvement would depend upon the intention of the person who collects or possesses the information.

7.6 Broad Discretion of Executive Organs to Designate Proscribed Terrorist Organisations

According to s 3 of the TA 2000, the Secretary of State can proscribe any organizations that is ‘concerned in terrorism.’ The Act sets out that an organisation can be considered as such if it ‘commits or participates in acts of terrorism,’ ‘prepares for terrorism,’ ‘promotes or encourages terrorism,’; or ‘is otherwise concerned in terrorism.’ Accordingly, the Secretary of State has wide discretion to designate terrorist organisations. The only restriction on that power is that the five discretionary

---


1154 TA 2000, S 3(4).

1155 TA 2000, S 3(5).
factors\textsuperscript{1156} should be considered and Parliament should assent to the proscription.\textsuperscript{1157} Both houses must support the proscription order for it to be passed, and it may not be amended in any way after being debated by Parliament.\textsuperscript{1158} Given this, the Parliament did not effectively review of Proscription order of the Home Secretory.

Additionally, Lord Carlile claimed that proscription is useful when dealing with low-level activities and prevents terrorist organisations from operating in the UK.\textsuperscript{1159} However, the role of the judiciary in terrorism proscription is limited. Indeed, no judicial involvement has been observed in the proscription process. The Court of Appeal has insisted that the Proscribed Organizations Appeal Committee (POAC) should apply an intense level of scrutiny to the Home Secretary’s decision to proscribe.\textsuperscript{1160} Moreover, compared to TPIMs, proscriptions are no longer reviewed annually. Instead, the Home Secretary will only consider de-proscription on application.\textsuperscript{1161} This will lead to proscriptions lasting indefinitely, not only because it is costly to apply de-proscription but also because it seems unrealistic that currently proscribed organisations would apply for de-proscription.\textsuperscript{1162}

There is no automatic legal scrutiny of proscription, and challenges to proscription

\textsuperscript{1156} The factors to be considered are:
(a) the nature and scale of the organisation’s activities;
(b) the specific threat that it poses to the UK;
(c) the specific threat that it poses to British nationals overseas;
(d) the extent of the organisation’s presence in the UK; and
\textsuperscript{1158} To be removed from Schedule 2 – to be deproscribed – requires direct application to the Secretary of State. If the Secretary agrees, she may lay an order before Parliament for approval. If the Secretary refuse, the organisation may appeal to the Proscribed Organisations Appeals Commission (POAC), which may only allow the appeal if it considers the Secretary’s determination flawed, subject to judicial review principles. Either the organisation or the Secretary may appeal POAC’s decision at the Court of Appeal, the decision of which is binding.
\textsuperscript{1160} Secretary of State for the Home Department v Lord Alton of Liverpool and others [2008] EWCA Civ 443, [2008] 1 WLR 2341, [38].
cases are almost unheard of. Proscriptions are not required to be reviewed periodically. And, to date, no proscribed organisation has been de-proscribed under the UK government’s annual review. It is worth noting that the Secretary of State is also in charge of the de-proscription. The decisions here could be referred to the Proscribed Organizations Appeal Committee (POAC) for appeal, at which point there would be full judicial scrutiny of the case.

Since 2001, all 12 applications to the Secretary of State for de-proscription have been refused. However, only one of these decisions was successfully appealed in the POAC in the case of Secretary of State for the Home Department v Lord Alton of Liverpool. The lack of successful de-proscription implies that the wide discretionary executive itself is reluctant to de-proscription. Accordingly, the realistic way to obtain de-proscription is recourse to the judiciary via the POAC, and it highlights the importance of the independent judicial review of executive decisions.

7.7 Aggravated Punishment for Terrorism-related Offences

Similar to China, E&W has a tendency of applying aggravated punishment for terrorism-related offences. Reiner argued that practices of punishment of terrorism precursor offences are often accompanied by ‘draconian’ sentences. Surprisingly, there has been very little research on the sentencing for terrorism-related offences.

1164 Ibid, para 4.23and 4.25.
1168 Lord Alton of Liverpool & Others (in the Matter of the People’s Mojahadeen Organisation of Iran) v Secretary of State for the Home Department, Proscribed Organisations Appeal Committee (POAC), Appeal No: PC/02/2006. The decision of the POAC was later upheld by the Court of Appeal in Secretary of State for the Home Department v Lord Alton of Liverpool[2008] EWCA Civ 443. <https://www.theguardian.com/politics/2020/may/20/uk-governments-new-counter-terrorism-bill-the-key-measures>, >29 Oct 2020.
Some scholars argue that the sentences for preparatory terrorism offences tend to be relatively high, often even higher than sentences for murder and sexual assault. As is the case in China, a “terrorism connection” has been an aggravating factor in E&W.

In addition, although there is an assumption that early intervention in criminal offences will result in lower penalties, sometimes ‘over-punitive’ sentences have been administered for preparatory offences that are far removed from the actual commission of terrorist acts. In E&W, concepts of punishment, deterrence, denunciation and incapacitation are prioritised in sentencing terrorism-related offences, which may lead to higher sentences. Many argue that there has been an excessive emphasis on deterrence and punishment.

For instance, heavy sentences have consistently been handed down for offences of possession and collecting terrorism information under s 57 and s 58. Since there is no fault requirement in s 57 and s 58, some people who have no terrorism purpose or involvement may still be convicted. Furthermore, the punishment under strict liability is harsh, with a maximum sentence of 15 years under s 57 and 10 years under s 58. Academic textbooks generally emphasise the culpability is necessary for the moral or legal requirement for criminal liability. Ashworth argued that the deprivation of liberty for an offence which does not require proof of culpability is disproportionate ‘since the seriousness of an offence is constituted partly by the defendant’s culpability; no fair foundation for imprisonment has been laid if culpability is not required as to a significant element in the offence.’

The principle of proportionality also implies that anti-terrorism laws must effectively and reasonably prevent expected damage. The basic test of proportionality is that the
punishment is proportionate with the crime. Both Home Secretary Charles Clarke\textsuperscript{1177} and Independent Reviewer Lord Carlile\textsuperscript{1178} held the view that the new offences in the TA 2006 were proportionate and in compliance with the HRA 1998. However, it has been argued that s 1 of the TA 2006 violates the principle of proportionality because the penalty is up to seven years' imprisonment regardless of whether the indirect encouragement actually results in the incitement of violence.\textsuperscript{1179} Furthermore, s 1 of the TA 2006 does not require an actual harmful effect, so the punishment could be considered disproportionate.

7.8 Enforcement of Anti-Terrorism Legislation

In order to prevent the anticipatory risks of cyberterrorism, the anti-terrorism laws are predominantly based on pre-emptive measures. For example, the executive is gradually granted extensive powers to investigate, detain and control suspected terrorists. However, the judiciary still plays an essential role in scrutinising these measures (e.g. repealing indefinite detention, and abolishing control orders and replacing it with TPIMs).

7.8.1 Expansion of Detention

Similar to China, one manifestation of E&W’s pre-emptive tendency in relation to counter-terrorism measures is the continuous extension of the detention period. The pre-charge detention period under the TA 2000 was extended from seven days to 14 days by the Criminal Justice Act 2003, and up to 28 days by the TA 2006.\textsuperscript{1180} Furthermore, the TA 2008 extended the detention period for terrorism-related suspects to 42 days. Detention without warrant was proposed to be extended to 90 days\textsuperscript{1181} in

\begin{itemize}
  \item \textsuperscript{1179} TA 2006, S 1.
  \item \textsuperscript{1180} TA 2006, S 41.
  \item \textsuperscript{1181} The public reacted strongly against this idea. See Alan Travis, British police powers toughest in Europe (The Guardian, 13 October 2005) <\url{https://www.theguardian.com/uk/2005/oct/13/terrorism.immigrationpolicy}> accessed 20 Oct 2020. See
\end{itemize}
the House of Commons, but this was met with strong opposition from the media and the public, and was finally dismissed by 322 votes to 291.\textsuperscript{1182} This proposed extension stirred fierce debate as to whether harsher measures to combat terrorism would be compromising human rights protection in order to safeguard national security. Some scholars\textsuperscript{1183} have claimed that there is no convincing case for such a lengthy pre-trial detention being reasonable. The United Nations Special Rapporteur on Human Rights and Counter-terrorism, Martin Scheinin, also severely criticised the bill, fearing that it would set a negative precedent for other countries.\textsuperscript{1184}

Moreover, partly in order to pursue the CONTEST strategy, E&W’s government has placed a greater emphasis on the use of detention to counter those suspected of connection to terrorism-related activities. Perhaps the most severe and controversial clauses in the ATCSA 2001 is the indefinite detention of a certified suspected foreign terrorist (s 21),\textsuperscript{1185} and where if the Home Secretary reasonably believes that a person (a non-British citizen) is an international terrorist, then the person will be issued a certificate, and will be detained indefinitely according to s 23.\textsuperscript{1186}

However, this provision was abolished following the landmark ruling in the case of \textit{A v Secretary of State for the Home Department}\textsuperscript{1187} (also known as the \textit{Belmarsh case}) by the House of Lords in 2005. This case prompted much discussion among scholars. Tomkins supported this decision, claiming that ‘it marks the beginnings of a much belated judicial awakening to the fact that even in the context of national security the

\begin{footnotesize}
\begin{enumerate}
\item M Scheinin stated: ”The United Kingdom has a long standing history of effective human rights protection, however I am concerned that this Counter-Terrorism Bill, if adopted, could prompt other states to copy the provision into their own counter-terrorism legislation, without reflecting on the importance of effective judicial review” see UN General Assembly, ‘Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while countering terrorism’ (2009) UN Doc A/HRC/10/3/Add.1.
\item ATCSA 2001, S 21.
\item ATCSA 2001, S 23.
\item \textit{A v Secretary of State for the Home Department} [2004] UKHL 56 [hereinafter “Belmarsh”]
\end{enumerate}
\end{footnotesize}
courts have a responsibility to ensure that the rule of law is respected.' 

Nonetheless, Feldman argued that, at the time 'it was unprecedented for UK judges to adjudicate on the legitimacy of measures adopted in good faith on national security grounds.' Lord Bingham used Strasbourg case law to demonstrate that executive authorities should have considerable discretion to determine whether an emergency exists. However, the *Belmarsh* decision ultimately ruled that detention without trial was disproportionate and discriminatory, and issued an incompatibility declaration under section 3 of the HRA. As a result of *Belmarsh’s* ruling, the Prevention of Terrorism Act 2005 abolished detention without trial and replaced it with the control order system, which included a series of criminal investigation-related restrictions.

7.8.2 Granting the Police Overbroad Stop and Search Powers

Under s 44, police are given the power to stop and search any vehicle or person in certain areas within their jurisdiction without any reasonable suspicion that the vehicle/person might be connected with terrorism. S 44 played a key preventive role in counter-terrorism strategy: the police preventively involved in stopping, questioning and searching suspect who posed a terrorist threat; the police maintained a pre-emptive function to prevent terrorists from carrying out terrorist acts.

However, s 44 stop and search is criticised for being overbroad, and has been condemned for violating Article 5 and Article 8 of the ECHR as it lacked the adequate legal safeguards against abuse. The police is empowered with wider discretion to

---

1190 Belmarsh, para. 28-9.
1192 Terrorism Act 2000, s 44(1).
1193 Terrorism Act 2000, s 45(1) (a).
1196 Gillan and Quinton v UK (2010) (Application no. 4158/05) at para 56,63.
gather evidence and intelligence to support the detention or release of a suspected
terrorist.\textsuperscript{1197} Moreover, the police was granted extensive discretion to collect
information in support of other non-criminal measures (such as control orders or TPIMs
and deportation), which are alternative measures applied to avoid having suspected
terrorists enter criminal proceedings.\textsuperscript{1198}

Furthermore, in the case of \textit{Gillian and Quinton v UK}, the ECtHR emphasised that in
order to be compatible with the rule of law, power must have adequate legal protection
against arbitrariness, and the scope of discretion and the way it is exercised must be
as clear as possible. According to Lord Lloyd of Berwick, the wide powers of s 44 (such
as covert surveillance, intelligence gathering and clandestine interference with terrorist
plots)\textsuperscript{1199} are intended to facilitate the authorities in fulfilling their duties to intercept
and suppress terrorism.\textsuperscript{1200} Some scholars have argued that these powers lack
transparency and accountability, and that they disregard human rights.\textsuperscript{1201} Turk
argued that reducing the legal constraints on the police’s anti-terrorism powers may
erode ordinary legal protection and lead to arbitrary detention.\textsuperscript{1202} Pertinently, the
\textit{Gillian and Quinton} case supports this argument.

Stop and search is ordinarily a primary tactic of policing, and during threats of terrorism
can form part of ‘high policing’ strategies which are adopted by the police during covert
surveillance, intelligence gathering and clandestine interference with terrorist plots\textsuperscript{1203}.

Lord Carlile QC expressed concern that s 44’s granting of broad powers to police may

\textsuperscript{1197} Especially following the London bombing in 2005, an unpopular side effect in the use of this power
was the majority of citizens stopped by the police were disproportionately of black or Asian ethnicity. A
Parmer, ‘Stop and Search in London: Counter-Terrorist or Counter-Productive?’ (2011)21 (4) PS 369, 370.
\textsuperscript{1198} WC Alister, ‘Risk Assessment, Counter-Terrorism Law & Policy; A Human Rights-Based Analysis:
Assessing the UK’s Pre-emptive and Preventive Measures of Countering Terrorism, Interaction with Article 5
and 6 of the European Convention on Human Rights, and the potential Role of Risk Assessment’ (DPhil
\textsuperscript{1199} D Weisburd, B Hasisi, T Jonathan and G Aviv, ‘Terrorist threats and police performance: a study of
Israeli communities’ (2010) 50(4)BJC 726.
\textsuperscript{1201} D Weisburd, B Hasisi, T Jonathan and G Aviv, ‘Terrorist threats and police performance: a study of
Israeli communities’ (2010) 50(4)BJC 726; DH Bayley and D Weisburd, ‘Cops and spooks: The role of
the police in counterterrorism’, in D Weisburd and others (eds), \textit{To Protect and to Serve: Police and
Policing in an Age of Terrorism – and Beyond} (Springer 2009) 81-99.
\textsuperscript{1203} D Weisburd, B Hasisi, T Jonathan and G Aviv, ‘Terrorist threats and police performance: a study of
Israeli communities’ (2010) 50(4) BJC 726.
lead to an abuse of power.1204 In addition, both Lord Carlile QC and David Anderson QC supported the repeal of s 44 in their independent terrorism review.1205 The court’s decision in the Gillan and Quinton case led to the then Home Secretary, Theresa May, declaring that the UK government no longer used s 44 because it did not provide sufficient safeguards to protect civil liberties.1206

7.8.3 Broad Discretion to Issue Control Orders

As noted above, the PTA 2005 abolished the provision permitting the indefinite detention of foreigners suspected of terrorism and replaced them with a new control order system.1207 The control order system supports the prevention pillar of the UK government's CONTEST strategy, which aims to enable control and management of the threat of terrorism.1208 Control orders were described under s1(1) PTA 2005 as order ‘against an individual that imposes obligations on him for purposes connected with protecting members of the public from a risk of terrorism.’1209 Those obligations were considered ‘necessary for preventing or restricting involvement in terrorism-related activity.’1210 S 1(4) lists a lengthy catalogue of restrictions on personal freedom, including restrictions on movement, access and communication.1211

The Home Secretary was empowered with the discretion to impose the obligations under the control order system. The orders are divided into two categories: ‘non-derogating’ and ‘derogating.’ Derogating orders were obligations imposed on individuals which would have such a significant impact upon the liberty of the individual that they would be incompatible with Article 5 of the ECHR. Non-derogating orders

---

1206 HC Deb 8th July 2010, vol 513, col 29.
1209 PTA 2005, s 1(1).
1210 PTA 2005, s 1(3).
1211 PTA 2005, s 1(4).
were obligations imposed on individuals by the Home Secretary which are compatible with Article 5 of the ECHR. MacDonald argued that this regime will address the issues of proportionality because the obligations imposed would be 'tailored to meet the threat posed by the particular suspect.'\textsuperscript{1212} Fenwick considered these obligations were less invasive of human rights compared to the previous indefinite detention.\textsuperscript{1213} However, Zender argued that the PTA 2005 did not provide a clear demarcation point between the restriction and deprivation of individual freedoms under Article 5 of the ECHR.\textsuperscript{1214}

The control order regime is subject to a certain degree of judicial involvement in the PTA 2005. John Yates supported this regime because he was considered that '[the] balance between the countering the threat whilst preserving the liberty of the citizen is of course for Parliament to decide and determine.'\textsuperscript{1215} However, Charles Clarke, the then Home Secretary, claimed that a lack of judicial involvement was justifiable because the primary responsibility of the UK government is to protect national security and the executive is fully responsible for the actions of Parliament.\textsuperscript{1216}

The JCHR insists that the UK government should accept and respect the judicial review responsibility for personal freedom, and that denying this responsibility in the name of national security represents a subversion of the principle of separation of powers.\textsuperscript{1217} Therefore, the UK government has reluctantly accepted judicial intervention when issuing control orders to deprive or restrict a person's freedom.\textsuperscript{1218}

It should be noted that the obligations imposed should be proportionate with the risks

\textsuperscript{1212} S MacDonald, ‘ASBOs and Control Orders: Two Recurring Themes, Two Apparent Contradictions’ (2007) 60(4) PA 601, 604.
\textsuperscript{1213} H Fenwick, 'Preventative anti-terrorist strategies in the UK and ECHR: Control Orders, TPIMs and the role of technology' (2011) 25(3) IRLCT 129.
\textsuperscript{1214} L Zedner, 'Preventative justice or pre-punishment? The case of control orders' (2007) 59 CLP 174-203.
\textsuperscript{1216} HC Deb 22 February 2005, vol 431, col 40.
of the terrorist activities that need to be prevented.\footnote{Walker explained that whilst the regime was considered ‘odious’ it remained an 'imperative [means] of responding to [the] anticipatory risk of terrorism...'}\footnote{Walker, ‘The Threat of Terrorism and the Fate of Control Orders’ (2010) 3PL 4, 7.} As Watkins explains: ‘control orders are flawed but [it is] equally clear that some controlling mechanism is required on potentially dangerous individuals.’\footnote{Watkins ‘Control Orders: The Beginning of the End?’ in S King, C Salzani and O Staley (eds) Law, Morality and Power: Global Perspectives on Violence and the State (BRILL 2020) 53-60.}

These control orders could be applied to UK citizens and foreign nationals without discrimination, which is quite different from the previous version of control orders.\footnote{Under s 4 of ATCSA 2001, the Minister of Interior was empowered to detention of foreign nationals suspected involved in terrorism who threaten Britain’s national security and who cannot be deported to their countries of origin.} The orders can be divided into derogating or non-derogating orders,\footnote{Derogating control orders are those that require a previous derogation from Art. 5 ECHR. Such orders can only be made by the High Court, upon application by the government.} depending on their severity, and the difference between them is the degree of derogation of human rights under Article 5 of the ECHR. Non-derogating orders are adopted by the Home Secretary, whereas derogating orders are issued by a court, on application of the Home Secretary.\footnote{The orders are widely applied and include house arrests, curfews, electronic tagging, restricting the use of communication devices (such as a computer, phone, or Internet), restricting access to others and travel bans.} The orders are widely applied and include house arrests, curfews, electronic tagging, restricting the use of communication devices (such as a computer, phone, or Internet), restricting access to others and travel bans.

The control order system demonstrates the coexistence of risks and uncertainties, diverting suspected terrorists from criminal procedures toward executive areas with constantly expanding power in the name of pre-emption.\footnote{According to Aradau and van Munster, the rationale underpinning control orders is to prevent risk by acting pre-emptively, before any harm can come to the State and its citizens.} It has been argued that control orders have imposed restrictions and obligations on

\footnotesize{\begin{itemize}
\item For instance, a suspect transferring money to a listed terrorist organisation might be subject to having his assets frozen.
\item Walker, ‘The Threat of Terrorism and the Fate of Control Orders’ (2010) 3PL 4, 7.
\item Under s 4 of ATCSA 2001, the Minister of Interior was empowered to detention of foreign nationals suspected involved in terrorism who threaten Britain’s national security and who cannot be deported to their countries of origin.
\item Derogating control orders are those that require a previous derogation from Art. 5 ECHR. Such orders can only be made by the High Court, upon application by the government.
\item PTA 2005, s 1(2).
\item PTA 2005, s 9.
\item N McGarrity and G Williams, ‘When extraordinary measures become normal; pre-emption in counter-terrorism and other laws’ in N McGarrity, A Lynch and G Williams (eds), Counter-Terrorism and Beyond: The Culture of Law and Justice After 9/11 (Routledge 2010) 131- 149.
\end{itemize}}
suspected terrorists but they are not found guilty of any offence. Zedner and Ericson argued that control orders allow the State to impose restrictions on suspects based on uncertainty without disclosing or exposing intelligence to the public.\textsuperscript{1228}

7.8.4 Terrorism Prevention and Investigation Measures (TPIMs)

In 2011, the control order regime was replaced by TPIMs. The purpose of introducing TPIMs was a ‘cautious rebalancing in favour of liberty.’\textsuperscript{1229} TPIMs are believed to provide a re-balance between national security and human rights, re-focusing on prosecuting suspected terrorists\textsuperscript{1230}, because doing so is an ‘institutional self-interest.’\textsuperscript{1231} TPIMs function as a means of early intervention to protect the public when there was not a ‘realistic prospect of conviction.’\textsuperscript{1232}

In addition, the Independent Reviewer, Macdonald, criticised the control order regime of obstructing prosecution.\textsuperscript{1233} This particular report recommended that TPIMs be created to re-align with the criminal justice system which aimed to facilitate the prosecution, conviction and punishment of terrorists. Accordingly, these measures are an alternative to criminal justice for those who cannot be prosecuted but pose a threat to national security.

According to the Terrorism Prevention and Investigation Measures Act 2011 (hereafter ‘TPIMA’), the Home Secretary must apply for permission from the courts to issue an individual with a TPIM notice.\textsuperscript{1234} The permission hearing can be conducted without

\begin{itemize}
\item \textsuperscript{1229} Helen Fenwick giving evidence before the Joint Committee on the Draft Enhanced Terrorism Prevention and Investigation Measures Bill (24th October 2012b) <http://www.parliament.uk/documents/joint-committees/Draft%20ETPIMS%20Bill/HC%20495%20iii%2024%20October%202012%20Corrected.pdf> accessed 19th Feb 2020.
\item \textsuperscript{1230} MacDonald Report, \textit{Review of Counter-Terrorism and Security Powers: A Report by Lord MacDonald of River Glaven QC} (Cm 8003, 2011)
\item \textsuperscript{1231} Joint Committee on Human Rights, \textit{Post-Legislative Scrutiny: Review of the Terrorism Prevention and Investigation Measures Act 2011, Tenth Report} (HL 113, HC 1014, 2013-14).
\item \textsuperscript{1232} B Middleton, ‘Rebalancing, Reviewing or Rebranding the Treatment of terrorist Suspects: The Counter- Terrorism Review 2011’ (2011) 75(3) JCL 225, 227; Also see Home Office, \textit{Pursue, Prevent, protect: The United Kingdom’s Strategy for Countering International Terrorism} (Cm 7547, 2009)
\item \textsuperscript{1233} MacDonald Report, \textit{Review of Counter-Terrorism and Security Powers: A Report by Lord MacDonald of River Glaven QC} (Cm 8003, 2011) 9.
\item \textsuperscript{1234} TPIMA, s 3(5)(a). An exception exists for cases in which the Home Secretary ‘reasonably considers that the urgency of the case requires terrorism prevention and investigation measures to be
the concerned individual being present at the court. If the court grants the permission, the TPIM notice could be issued and a review hearing could be held where a Special Advocate represents the interests of the individual concerned. According to schedule 1 of the Act, the TPIM notice may contain any of the 12 types of measures, which are deemed necessary to prevent or restrict the individual's involvement in terrorism-related activity, such as 'an overnight residence measure, an exclusion and/or movement directions measure and an electronic communication device measure.' Once the TPIM notice is issued, it is valid for one year. If the statutory conditions are still met, the Home Secretary may renew it for a second year. However, the Home Secretary could only issue a new TPIM notice at the end of the second year if the statutory conditions are still met. Due to the relatively low frequency of application of TPIMs, according to the recommendations of the then independent reviewers, the Counter-Terrorism and Security Act 2015 made some amendments to the TPIMA.

The appellate courts' decisions have changed or repealed many anti-terrorism laws because the protection of individual liberties took precedence over national security. Meanwhile, these changes are also due to the decision of the UK's appellate courts' recognisance of the ECHR. As mentioned above, the evolution went from indefinite detention to control orders and then to TPIMs. Notably, in the case of Secretary of State for the Home Department v AP, the UK Supreme Court's decision emphasised that the interests of individual liberty prevailed over national security so the Court held that the 2005 Act violated Articles 5 and 8 of the ECHR. As a result, the control order regime in the PTA 2005 was repealed and replaced with TPIMs.

---

imposed without obtaining such permission’ (s 3(5)(b)).

1235 TPIMA, s 6(4).
1236 TPIMA, s 8(4).
1237 TPIMA, s 3(4). The other eight types of measure are: travel measure; financial services measure; property measure; association measure; work or studies measure; reporting measure; photography measure; and, monitoring measure.
1238 TPIMA, s 5(2).
1239 TPIMA, s 3.
Pursuant to section 3 of the HRA 1998, allowing the appellate court to declare statutory provisions inconsistent with the ECHR is a significant move towards the overthrow of parliamentary statutes in the judiciary. The introduction of this measure has to some extent kept the UK’s anti-terrorism-related executive powers in check by the judiciary. For example, UK courts have held that 18-hour curfews in control orders were seen as excessive and disproportionate, therefore violating Article 5 of the ECHR. 1242 Therefore, the UK courts did in effect force Parliament to change the law.

7.8.5 Tendency of Using Non-criminal Methods of Disruption to Deal with Preparatory Cyberterrorism Activities

Non-criminal disruption methods are applied to suspected terrorists who cannot be prosecuted. The reasons why these suspects involved in terrorist activities cannot be prosecuted include the following: insufficient evidence (especially given that intercepted evidence cannot be used in criminal trials1243); incriminating evidence not being disclosed for the sake of the public interest (e.g. to retain the cover and ensure the safety of human agents); and the individual having already served their sentence is still however assessed as a threat to national security.1244 Given this situation, there is a tendency to use non-criminal disruption methods to deal with cyberterrorists’ preparatory acts for prevention purposes.1245 This is similar to the use of administrative detention under China’s anti-terrorism law to combat preparatory terrorist acts.

TPIMs are ‘a useful tool for the protection of the public in exceptional cases where a credible terrorist threat cannot be dealt with by prosecution or deportation.’ 1246 Meanwhile, these measures should not be excessively relied upon. After all, TPIMs are ‘restrictive measures [which] should be imposed only when unavoidable, and as a

1242 Secretary of State for the Home Department v J.J. and others [2006] EWHC 1623 (Admin).
1243 Home Office, Intercept as Evidence (Cm 8989, 2014).
1244 S Macdonald and L Carlile, ‘Disrupting Terrorist activity: What are the limits to criminal methods of disruption?’ in SS Juss(eds), Beyond Human Rights and the War on Terror (Routledge 2019) 126.
1245 The CONTEST advocates the use of other methods of disruption that sit outside the criminal justice process.
last resort.’ 1247 With this in mind, the following concerns persist regarding these measures:

(1) The preconditions of the Home Secretary issuing a TPIM notice include that the individual is, or has been, involved in terrorism-related activity and that it is necessary to apply the measure to protect the public from terrorism. 1248 This risk assessment depends on both a forward-looking necessity evaluation and a backward-looking facts. 1249

(2) The second set of concerns focus on the roles of the executive and judiciary issuing TPIMs. Stuart proposed that the courts, rather than the executive, should issue TPIM notices. 1250 The underlying rationale of such concerns is that TPIMs will affect individual freedom and judicial independence. Some opine that in order to reduce the risk of endangering national security, TPIMs should be the responsibility of executive agencies operating with high efficiency and practical flexibility, and emphasise that the Home Secretary is best placed to make the decision to impose a TPIM notice. 1251 Currently, there seems to be a compromise between these two views—the Home Secretary issues TPIM notices after obtaining the permission of the courts.

(3) The third set of concerns regards the use of closed material proceedings. In order to prevent the disclosure of information to damage the public interest, the court may exclude the individual and his legal representative from the proceedings during both a TPIM review hearing and an appeal to the POAC. 1252 In addition, the right of individuals to communicate with their representatives is limited regarding closed materials. 1253 The Special Advocates claim that this restriction of communication with

---

1247 Ibid.
1248 TPIMA, s 3(1), 3(3)
1253 During closed sessions the individual is represented by a Special Advocate (a practitioner with security clearance appointed by the Attorney General). Before the Special Advocate is shown the closed materials he may communicate freely with the individual and the individual's legal representative. Once the Special Advocate has been served with the closed materials, the individual may still communicate with him (in writing and through his legal representative). But the Special Advocate may no longer
individuals will greatly limit their ability to operate effectively. They also point out that closed materials proceedings ‘are inherently unfair; they do not “work effectively”, nor do they deliver real procedural fairness.’

7.9 Conclusion

When looking at how to apply the existing anti-terrorism laws to combat cyberterrorism acts in E&W, we note there are two tendencies: from the substantive law perspective, E&W has adopted a pre-emptive approach to prevent the anticipated risks of terrorist attacks, manifested by a vague and overbroad definition of terrorism, proliferation of new offences, strengthening of punishment, broad discretion to designate terrorists, expansion of pre-trial detention and executive powers in general, and the use of non-criminal measures to achieve a repressive effect that is similar to that of criminal law measures.

Furthermore, through the critical examination of the existing anti-terrorism legislation with respect to basic criminal law principles, it could be concluded that E&W has showed a certain degree of arbitrariness when fighting cyberterrorism, and it has tended to emphasise national security over human rights protection from the perspective of substantive law and policy. However, as a rule of law jurisdiction, E&W still has a certain amount of respect for due process and human rights protection, driven by its independent judicial reviews and independent scrutiny of commissioners and parliamentary committees, so there are certain restrictions on state power to avoid becoming a rule by law jurisdiction. Furthermore, there are some striking similarities and differences in the legal responses to cyberterrorism between China and E&W, which will be demonstrated in the comparative chapter.

---

1254 Secretary of State, *Justice and Security Green Paper: Response to Consultation from Special Advocates* (Cm 8194, 2011) para. 27.
1255 Ibid, para.15.
Chapter 8 Comparative Analysis

8.1 Introduction

Through an examination of the legal systems of China and E&W in previous chapters, some difference were observed especially with respect to their legal systems, which are based on “rule of law” and “rule by law” respectively.1256 Meanwhile, through examining anti-cyberterrorism legislation and enforcement, a horizontal comparison of the legal responses of these two jurisdictions revealed some similarities as well as differences.1257 In light of this, we now delve further into the analysis of the relationship between these legal systems and the corresponding legal responses to cyberterrorism.

Examining the links between the legal regime and anti-cyberterrorism approach, this chapter argues that despite the differences in their legal systems, there are some convergences in the ways China and E&W respond to cyberterrorism, and that therefore legal responses to cyberterrorism are arguably contingent on the nature of the given legal system.

As demonstrated in previous chapters, there are various ways in which legal responses to cyberterrorism differ in China and E&W, and these differences are attributable to the differences in their legal and political systems. Specifically, E&W’s legal system is based on the rule of law, which includes supremacy of law, separation of powers, independent judiciary, and the protection of individuals’ fundamental rights. Accordingly, its anti-terrorism approaches are subject to judicial review, independent review, and legislative scrutiny. On the contrary, in China’s authoritarian political context, its legal system is based on rule by law, which implies the supremacy of the CCP, a concentration of powers, a lack of an independent judiciary, and a lack of human rights protection. Therefore, based on the differences between the two legal regimes, we would expect different legal responses to cyberterrorism. The divergences emerging from the examination of anti-cyberterrorism legislation and enforcement are

1256 The details of legal systems in E&W and China, see Chapter 4 and 6.
1257 The details of legal responses to cyberterrorism in E&W and China, see Chapter 5 and 7.
mainly as follows:

- Firstly, China and E&W have differences in their independent judicial review of terrorism-related cases.
- Secondly, there is a difference in legislative scrutiny and the independent review system in both jurisdictions.
- Thirdly, the safeguards for suspected terrorists’ rights are quite different in both jurisdictions.
- Fourthly, these two jurisdictions have differences in the human rights protection afforded to individuals in terrorism-related cases.

However, upon closer analysis, there are also a number of similarities in their approaches, suggesting that the nature of the legal system does not exclusively shape legal responses to cyberterrorism. Specifically, the main commonalities here could be divided into the following three categories:

(1) Substantive counter-terrorism laws

- Emphasis upon prevention and a pre-emptive tendency to combat cyberterrorism.
- Lack of a specific definition of “cyberterrorism” but a reliance upon a very broad and vague definition of terrorism, which could violate legal certainty and clarity, whilst enabling arbitrary law enforcement.
- Criminalisation of a wide range of terrorism precursor offences, with a tendency to extend criminal liability, early intervention, and erosion of basic criminal law principles.
- Both jurisdictions empower the executive organs with broad discretion to designate proscribed terrorist organisations.

(2) Procedures for enforcing counter-terrorism laws

- The vast majority of anti-terrorism laws gradually extend executive powers to interrogate, detain and control suspected terrorists during preliminary
investigation or pre-charge periods.

- Similar tendency of using non-criminal disruption methods to deal with preparatory cyberterrorism acts.

(3) Punishment of terrorism offences

- In both jurisdictions, a “terrorism connection” serves as an aggravating factor, which means terrorism-related offenders shall be given severer sentences.

This chapter begins by arguing that there are fundamental differences in the legal responses to cyberterrorism in China and E&W, which is unsurprising given their different legal and political systems. However, interestingly, there are also a number of commonalities emerging from the critical analysis of their approaches in the following section. Therefore, it will be concluded that the substantive relations of connection between legal systems and legal responses to cyberterrorism are not necessary but contingent because both ‘rule by law’ and ‘rule of law’ systems produce the same problems with regard to legal responses to cyberterrorism: ill-defined, disproportionality, uncertainty, arbitrariness, expansion of executive powers. This is because there are other key causal mechanisms at play, such as the need to adapt legal responses to the kind of fast-moving, potentially catastrophic and cross-jurisdictional threats generated by the hyperconnectivity of the World Wide Web and epitomised by the problem of ‘cyberterrorism.’ This could also stimulate a number of conjectures for further research regarding what other factors could explain these convergences and divergences, which will be demonstrated in the concluding chapter.

8.2 Divergence of Legal Responses to Cyberterrorism in China and E&W

Through a critical analysis and comparison of the legal responses to cyberterrorism, a list of divergences in the legal response to this problem could be identified in China and E&W. It could be argued that these divergences are attributed to the differences in legal systems rather than other possible drivers of the response to cross-jurisdictional problems such as cyberterrorism. The details of this analysis show as follows.
8.2.1 Differences in the Independent Judicial Review of Terrorism-related Cases

The first essential difference in the legal responses to cyberterrorism in China and E&W relates to the independent judicial review power of the court in terrorism-related cases. Manifestations of these divergences have emerged as follows.

(1) A huge difference regarding the de-proscription of terrorist organisations exists between these two jurisdictions. In E&W, the POAC has the power to review proscription and de-proscription cases. On the contrary, in China, the judiciary has the power to designate terrorist organisations, but that does not mean that it can review the results of the designations by the administrative organs. There is no independent review or supervision undertaken by other departments with regard to the designation mechanism in China. This highlights the importance of independent judicial review of executive decisions. In terms of the relevance of a legal regime to a legal response, this implies that divergence in the role of the judiciary in reviewing the executive decisions result in different outcomes of proscription and de-proscription in both jurisdictions.

(2) In terms of control order schemes, the biggest difference is in the permission procedures. In China, according to the supervision measures, control orders should be approved by the ‘the head of public security organ at or above the county level.’ This means that only the police (head of public security organs) in China have the power to issue control orders, without the supervision of judiciary departments. Meanwhile in E&W, non-derogating control orders are issued by the Secretary of State, with the permission of a court. The Secretary of State may issue urgent control orders without the permission of a court, however he/she must immediately refer it to a court, with hearings to commence within seven days of the making of the order. Therefore, the function of the court here is one of judicial review to decide whether to quash the order or one or several of its obligations, or give directions to the Secretary of State for the revocation or modification of the terms of the order. It could be argued that

---

1258 Prevention of Terrorism Act (PTA) 2005, s 3(3) and (4).
1259 B Jaggers, ‘Anti-Terrorism Control Orders in Australia and the United Kingdom: A Comparison’
E&W’s control order regime is subject to tighter scrutiny or safeguards, particularly surrounding human rights protections. In contrast, China’s control order regime lacks any internal or external scrutiny or safeguards.

(3) The judicial involvement of non-criminal disruption methods in China and E&W is also different. In China, the ambit and application of administrative detention, as is the case with restrictive measures, is not scrutinised by a judicial review process nor is it open to procedural checks and balances, except for the right of the detained to apply to the same decision-maker for reconsideration. This unconstrained and unsupervised discretion may result in police arbitrariness and abuses of power. From the pre-emptive point of view, the elastic utility of administrative detention is consistent with the prevention of the occurrence of substantial terrorist acts. More markedly, administrative detention extends the reach of the Criminal Law to penalise similar acts with a lower level of harm and severity in the domain of police powers.

In E&W, despite limited judicial involvement, there is still a certain degree of judicial review in the process of issuing TPIMs and control orders. For example, the Home Secretary issues TPIM notices after obtaining the permission of the court. Such permission hearings can be conducted without the concerned individual being present in the court. If the court grants the permission, the TPIM notice can be issued and a review hearing could be set, where a Special Advocate represents the interests of the individual concerned.

In addition, the Belmarsh case represents a landmark ruling regarding the judicial involvement of indefinite detention without trial. It was held that the detention without trial scheme was disproportionate and discriminatory, and issued an incompatibility declaration under section 3 of the HRA. As a result of the Belmarsh ruling, the Prevention of Terrorism Act 2005 abolished detention without trial and replaced it with

---


1260 CTL, Art. 53.
1262 TPIM, S 6(4).
1263 TPIM, S 8(4).
the control order system, which included a series of criminal investigation-related restrictions.\textsuperscript{1264}

As previous chapters have demonstrated, both China and E&W embrace the principle of judicial independence, but their interpretations of this principle are very different. In E&W, judicial independence is based on the rule of law and the separation of powers. The judicial power is vested in judges who are independent and subject only to the law. Judicial independence in E&W protects the judiciary from infringements by the legislative and executive branches, and constitutes a bulwark against any abuse of power. Meanwhile, in China, due to the centralisation of power, Chinese judges do not enjoy substantial independence and there is much room for political interference.

Generally, courts should be particularly vigilant so that governments do not exceed their legal authority and guarantee their citizens’ rights to the greatest extent. Chapter 7 assessed some court decisions, which determined whether anti-terrorism laws were in compliance with human rights laws and ultimately led to legislative changes, such as the TPIMs replacing control orders. This emphasises the importance of the judiciary checking and balancing the legislator in the context of countering terrorism. Therefore, it may be argued that the legal response to cyberterrorism in China has substantially diverged from that of E&W (over the course of the historical period covered by this thesis) and that lack of judicial independence from the executive is a key factor explaining this divergence.

\textbf{8.2.2 Differences in Legislative Scrutiny and Independent Review System}

China's legal responses to cyberterrorism has substantially diverged from E&W’s approaches as the former lacks legislative scrutiny and an independent review system regarding anti-terrorism legislation.

(1) It brings us a particularity for E&W which is quite different from China in this regard

as the former’s specific anti-terrorism laws have always been reviewed by an independent reviewer. Although the UK government is not forced to consider these reviews, past successful experiences have shown on many occasions that it did. The reports of the independent reviewer provide a valuable additional resource that informs the work of relevant committees. For instance, the PTA 2005 includes the appointment of an Independent Reviewer of Terrorism Legislation (e.g. Lord Carlile of Berriew) who is required to report nine months after royal assent, and then annually on the operation of control orders. The independent reviewer has a similar role when it comes to other pieces of legislation, namely the TA 2000 and the TA 2006. The role of the independent reviewer is crucial, as the annual reports may provide the basis for the committees’ scrutiny. For example, the independent reviewer of legislation, in a detailed report, indicated that the definition of terrorism remains broadly fit for purpose, not least because terrorism investigations require earlier intervention than conventional criminal investigations.

(2) In addition, the anti-terrorism legislation is subject to legislative scrutiny as established by Parliament in E&W. For instance, select committees play an important role in the scrutiny of counter-terrorism legislation: the Joint Committee on Human Rights (JCHR) has provided reports on a panoply of terrorism-related powers, including indefinite detention, pre-charge detention, and control orders. These reports often inform debate in Parliament during the passage and/or renewal of

\[1265\] See Chapter 6.
\[1268\] Lord Carlile, The Definition of Terrorism (Cm 7052, 2007) 48. Note that the government did not adhere to all of Lord Carlile’s recommendations.
\[1269\] House of Commons Standing Order 152B.
relevant provisions and, therefore, can influence voting in the House, perhaps against the Government.\textsuperscript{1273} For example, detention without warrant was proposed to be extended to 90 days in the House of Commons, but this was met with strong opposition from the media and the public, and was finally dismissed by 322 votes to 291.\textsuperscript{1274} Moreover, the E&W’s PTA 2005 includes a requirement for quarterly reporting to Parliament by the Home Secretary on his/her exercise of the control orders powers for the preceding three months.\textsuperscript{1275} Moreover, terrorism-related legislation subject to parliamentary review once enacted could be subject to post-legislative scrutiny. The committees may be required to report on implementation within one or several years after the enactment of the legislation in order to re-evaluate its effectiveness and impact. While a 3-5 year review of legislation was established in 2008,\textsuperscript{1276} this is unsuitable for some counter-terrorism elements given the pace of legislative change here.

On the contrary, China's anti-terrorism laws lack such an independent review system, and also lack the supervision of the judiciary and legislature. China is an authoritarian state in which a strong central government and administrative divisions exercise power on its behalf. Unlike E&W, the division of state organs (such as the executive branch, judicial branch, legislative branch, and supervisory branch) emphasises the differentiation of responsibilities, rather than the separation of powers.\textsuperscript{1277} According to the CTL, the departments related to counter-terrorism prefer cooperation over supervision and restriction of power.\textsuperscript{1278}

In addition, China has not introduced the western substantial separation of powers. Instead of separation of powers, China applies \textit{democratic centralism (minzhu}{\textsuperscript{1273}} See, for example, the government’s defeat with regard to the proposed extension to pre-charge detention beyond 42 days, following the report of the JCHR (JCHR, \textit{Nineteenth Report of Session 2006-07, Counter-Terrorism Policy and Human Rights: 28 days, intercept and post-charge questioning} (HL 157 HC 394, 2007)).

\textsuperscript{1274} See Chapter 7, section 7.4.1.

\textsuperscript{1275} Home office, \textit{Memorandum to the Home Affairs Committee: post-legislative assessment of the Prevention of Terrorism Act 2005} (Cm 7797, 2010).

\textsuperscript{1276} House of Commons, \textit{Post-Legislative Scrutiny: The Government’s Approach} (Cm 7320, 2008).


\textsuperscript{1278} Art.8 of CTL states that all kinds of anti-terrorism related departments should implement a work responsibility system based on division of labor.
The legislative organ, the National People’s Congress, is nominally the highest state power, which generates and supervises the other two state powers. However, in reality, the power of these three state organs is ultimately concentrated in the hands of the CCP. With regard to the implication of counter-terrorism legal approaches, China lacks effective judicial review and checks and balances to prevent abuses of state power and arbitrariness, thereby leading to unrestricted violation of individual rights.

8.2.3 Different Protection of Suspects’ Rights in Terrorism-related Cases

Another significant divergence in the legal responses to cyberterrorism in China and E&W is reflected in the protection of suspects’ rights during detention, interrogation, and control of suspects in China and E&W. China lacks procedural rights protection for suspects and due process in terrorism-related cases, mainly manifested as follows:

(1) There is a huge difference in the admission of intercept or intelligence-based evidence in criminal trials in these jurisdictions.

In E&W, intercept and intelligence-based evidence cannot be used in criminal trials, under the s 17 of the Regulation of Investigatory Powers Act 2000 (RIPA 2000). However, the UK government might have a move to relaxing the ban on some uses of intercept evidence.

In order to overcome the relatively large obstacle of prosecution in terrorism cases, the use of intercept evidence in criminal trials has stoked huge controversy. This debate has revealed acute tensions between individual and national security interests. The

---

1279 According to the Chinese Constitution, all state power belongs to the people and must be exercised through the NPC and local people’s congress at various levels (Art.2). “Democratic centralism (minzu jizhong zhi)”, rather than separation of powers, is a guiding principle of the Constitution. Under the principle of “democratic centralism”, the NPC is the highest organ of state power (Art.57). The central government (State Council) and the two supreme judicial authorities (the SPC and the SPP) are therefore generated and supervised by the NPC.


former Independent Reviewer of Terrorism Legislation, Lord Carlile, argued that the admission of intercepted evidence was not the 'silver bullet', and might compromise the criminal trial. However, an increasing number of people (senior security officers, police chiefs, NGOs, and the JCHR) are in favour of accepting intercept evidence.

In China, although the legality of technical investigation has come under question because of the ambiguity of its applicability, according to the Criminal Procedural Law (CPL), material collected through technical investigation measures is considered valid, which as the incriminating evidence against suspects in the court. Therefore, it is indisputable that intercept evidence is allowed in criminal trials regarding terrorism cases in China.

(2) China and E&W have different safeguard of suspects’ rights in terrorism-related cases.

In China, as police powers continue to expand, suspects in terrorism-related cases do not enjoy that full legal rights that would ensure equal litigation capacity in criminal justice procedures. For example, suspected terrorists are limited in accessing legal counsel during the investigation phase. Furthermore, according to the CTL, there is no judicial involvement in the police issuance of control orders, and no procedural safeguards seem to exist during this process in China. The legislator completely ignores the right of the controlled person to obtain legal counsel, and there is no checks and balances mechanism in the law that could supervise the control order. Moreover, neither the CTL nor the CPL provides a remedy system for an independent and impartial review of the legality of the order issued by the police.

1285 See Chapter 5, section 5.9.2.
1286 Article 33 of the 2012 Criminal Procedure Law, details see Chapter 5, section 5.9.
In E&W, according to the Terrorism Prevention and Investigation Measures Act 2011 (hereafter ‘TPIMA’), the Home Secretary must apply for permission from the court to issue an individual with a TPIM notice.1287 The permission hearing can be conducted without the concerned individual being present in the court.1288 If the court grants permission, the TPIM notice could be issued and a review hearing could be scheduled, where a Special Advocate represents the interests of the individual concerned.1289 The Special Advocate is shown the closed materials and he/she may communicate freely with the individual and the individual’s legal representative.1290 In addition, although the procedural justice in control order hearings has been questioned,1291 the suspects still receive certain protections to ensure fairness. For example, a person subject to a control order can apply for its revocation or variation when it is up for renewal by outlining reasons in writing to the court in E&W.1292

8.2.4 Differences in Human Rights Protection

The different understandings of human rights protection in China and E&W is also a significant factor leading to different legal responses to cyberterrorism in the covered jurisdictions.

(1) lack of Human Rights Act in China

In China, the human rights values explicitly granted by the Constitution are restricted.1293 Therefore, the understanding of human rights in China is rather obligation-based, which means individual rights are considered subordinate to the

---

1287 TPIMA, s 3(5)(a). An exception exists for cases in which the Home Secretary ‘reasonably considers that the urgency of the case requires terrorism prevention and investigation measures to be imposed without obtaining such permission’ (s 3(5)(b)).
1288 Ibid, S 6(4).
1289 Ibid, S 8(4). The Special Advocate is a practitioner with security clearance appointed by the Attorney General.
1292 Ibid.
1293 Chinese Constitution Code, Art.51: “Citizens of the People’s Republic of China, in exercising their freedoms and rights, may not infringe upon the interests of the state, of society or of the collective, or upon the lawful freedoms and rights of other citizens.”
needs and demands of national interests and social stability. China’s basic stance on the development of human rights is to prioritise people’s rights to subsistence and development, making development the principal task ahead of promoting citizens’ political, economic, social and cultural rights.\textsuperscript{1294}

With the development of globalisation and China’s integration into the world order, the country is under pressure to deal with terrorism in accordance with international human rights law. In response, it has published documents on the human rights situation in Xinjiang\textsuperscript{1295}, three national human rights action plans and corresponding reviews\textsuperscript{1296} as well as a report on the implementation of the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment,\textsuperscript{1297} all of which demonstrates that the CCP has made some effort to reduce human rights violations and ensure due process. The latest national human rights action plan envisions restrictions of the executive power and improved mechanisms against torture and illegal internment by 2020.\textsuperscript{1298}

Unlike other democracies, the UK has no written constitution to guarantee its citizens’ rights. So, in E&W, the passage of the Human Rights Act 1998 (HRA 1998) was a crucial step toward protecting individual rights. It incorporated the rights provided for under the European Convention on Human Rights (ECHR).\textsuperscript{1299} Basic human rights include freedom of thought, expression and religion, freedom of assembly and

---


\textsuperscript{1298} A recent example of the CCP’s efforts to improve the participation of ethnic minorities can be seen from the National Human Rights Action Plan (2016-2020) [国家人权行动计划 (2016-2020)], <http://www.xinhuanet.com/politics/2016-09/29/c_129305934_5.htm. > accessed 20 Sep 2020.

\textsuperscript{1299} G Slapper and D Kelly, The English legal system (13th edn, Routledge 2012) 45, 74.
association, the right to fair trial, the right to enjoy possession, and the protection of property. These rights also indirectly restrict legislative and executive authorities.  

(2) The court has no power to review anti-terrorism legislation and enforcement in the name of human rights protection in China. 

Indeed, in China, the court has no power to review government violations of human rights in accordance with the Constitution, nor does an independent institution review the state organs’ compliance with the Constitution, and no citizen has the right to require a decision by court or any other state organisation on the basis that its human rights have been violated.

In E&W, the implementation of the HRA 1998 did not abolish the principle of parliamentary sovereignty, but the Act had the potential to create frictions between the judiciary, the legislative and the executive. Although the court may not declare the primary legislation invalid (parliamentary supremacy), the Act gives the court extended interpretative power. In particular, it is necessary to read and interpret statutes in conformity with the human rights incorporated in the HRA 1998. Therefore, the court may challenge parliamentary sovereignty by declaring the incompatibility of the legislation. Therefore, the HRA 1998 proposes a compromise scheme that leaves the final decision to Parliament, but gives the court the power to influence its decision.

There is no uniform standard universally applied to regulating individual rights, and the extent to which state organs and citizens are restricted. So, this arduous task has been left to the courts. Especially in the context of counter-terrorism, individual rights in both

---

1301 Therefore, Zhang Qianfan suggests the establishment of an independent committee under the NPC. See, K Blasek, *Rule of Law in China: A Comparative Approach* (Springer 2015) 51.
1302 See Chinese Legislation Law, s 90 par. 2: any citizen can only suggest the SCPC to deal with a certain issue or critic on legislation. But the actual dealing or decision cannot be claimed by citizens.
1303 The principle of sovereignty/supremacy of parliament is seen critical by C Elliott and F Quinn, *English Legal System* (13th edn, Pearson Essex 2012)
1305 S 3 of the HRA 1998 requires all legislation to be read, to give effect to the rights provided under the ECHR.
China and E&W have been derogated. There is a creeping erosion of liberty taking place through the passing of numerous expansive anti-terrorism acts—each of them seems harmless, but they add up to a ‘formidable armory of state powers’.\textsuperscript{1308} The biggest difference between China and E&W is still the role of the court. China does not have a constitutional court, which means that judges cannot directly invoke the Constitution when ruling, so they cannot examine whether legislation and administrative acts are in compliance with the Constitution to protect human rights.

An important difference between the control order schemes of China and E&W is that the latter’s scheme is built around the HRA 1998 and the UK’s obligations to the ECHR. However, China has no dedicated human rights legislation.

(3) There are also differences between the two jurisdictions in terms of the priority attached to national security and human rights in anti-terrorism legislation and enforcement.

Both China and E&W have to face the challenge of how to strike a proper balance between security and liberty in dealing with cyberterrorism. Balancing security and freedom in the context of counter-terrorism has been the subject of long-standing discussions in officialdom and academia.\textsuperscript{1309}

With respect to the protection of human rights, we have noted in general two interesting developments in both China and E&W: firstly, anti-terrorism legislators in both jurisdictions have shown a growing tendency to ignore human rights, putting security first. However, at the level of judicial practice, there has been some divergence in the two jurisdictions’ development, in E&W courts revoke laws for not being reconcilable with human rights. For instance, the appellate courts’ decisions have changed or repealed many anti-terror laws because the protection of individual liberties took precedence over national security. As a result, the court held that the control order regime violated Articles 5 and 8 of the ECHR, which was repealed and replaced with TPIMs. In China, there is no such result because the judiciary cannot review legislative

\textsuperscript{1308} J Alder, Constitutional and administrative law (7th edn, Palgrave Macmillan 2009)377.
\textsuperscript{1309} See Chapter 7, section 7.3.
and enforcement agencies.

E&W still has a certain degree of individual rights protection through judicial review, which is a substantial constraint on any potential misuse of state powers. On the contrary, in China, although the policy slogan and legal provisions emphasise the protection of human rights, it is still just rhetoric. Therefore, the different judicial review system is a significant driving force behind the divergence of human rights protection in the context of combating cyberterrorism.

(4) The different relationship between scholars and the government

There is a closer link between state and scholars in China than there is in E&W. This limits Chinese academic criticism of existing legal responses to cyberterrorism. Most scholars function to justify China's counter-terrorism policies and legal responses, rather than critically challenging the existing authority and problems, so that their studies function to reinforce the existing anti-terrorism strategy. For example, with regard to legal responses to terrorism issues, many scholars accept the official discourse without criticism, leaving issues such as human rights violations unaddressed. Although some Chinese scholars have tried to criticise some issues related to counter-terrorism, such as criticism of the principle of ‘combining leniency with severe punishment,’1310, ‘pocket crime,’1311, and ‘the hard approach,’1312 these criticisms have not been enough to influence the CCP to change its anti-terrorism laws.

In contrast, British scholars often criticise existing anti-terrorism legislation and enforcement, such as the vague and overbroad definition of terrorism, the wide range of terrorism-related precursor offences, the negative impact of human rights and rule of law due to expanding the application of the existing criminal law, and facilitating early intervention to increase security against terrorism.1313 This thesis mainly focuses on

---

1313 The details of criticism of existing approaches to anti-terrorism could be found in the Chapter of
the tension between expanding the scope of terrorism-related offences, facilitating early intervention to prevention and rule of law values, and human rights protection. Meanwhile, some of the literature has proposed that legislative restrictions should be imposed on anti-terrorism powers.\textsuperscript{1314} Moreover, in many Western jurisdictions such as E&W there has been a clear tendency toward the intensification of laws and punishments in relation to terrorism during the post-2001 era.\textsuperscript{1315} More specifically, stringent legislation has been gradually enacted to criminalise a series of terrorism-related acts, and harsh criminal measures are increasingly being applied to control and punish terrorists.

In sum, the approaches of both China and E&W to cyberterrorism may lean towards rule by law. However, due to legal constraints such as an independent judiciary, independent review, and legislative scrutiny in E&W, the latter still maintains the rule of law to the maximum extent, restricting the state power and protecting citizens’ rights to a certain extent. In contrast, due to the deep-rooted supremacy of the CCP and the authoritarian political context, although China has made some efforts to legitimise its anti-terrorism approaches (such as the adoption of a double-track designation system, combining leniency with severe punishment policy), it has imposed no substantive internal and external restrictions because of a lack of basic rule of law principles (such as separation of powers, independent judiciary and supremacy of law), which leads to the arbitrariness of state power.

8.3 Convergence of Legal Responses to Cyberterrorism in China and E&W

From the above analysis, there are clearly many differences between China and E&W in their legal approaches to cyberterrorism, which suggests that the relationship between the legal system and legal responses to cyberterrorism should be necessary. However, through further comparative analysis, we observe that the legal responses

\textsuperscript{1314} Details could be found in Literature Review Chapter.
\textsuperscript{1315} For a detailed discussion of counterterrorism strategies in Western democracies, see Andrew Lynch, Nicholas Mcgarrity and George Williams, Counter- Terrorism and Beyond: The Culture of Law and Justice After 9/11 (2012).
to cyberterrorism of China and E&W have been becoming more convergent, which implies that the substantive relationship between the legal system and the legal responses of China and E&W is contingent in the context of combating cyberterrorism.

### 8.3.1 Preventive and Pre-emptive Tendencies

The comparison of the two legal regimes indicated that despite the different understandings of the rule of law, there appear to be some convergences with respect to legal responses to cyberterrorism. Indeed, both China and E&W have similar rule by law tendencies in the context of combating cyberterrorism. Such imprecision in “rule by law” is underpinned a more authoritarian approach, which is justified in terms of the need for more ‘preventive’ or ‘pre-emptive’ interventions against online preparatory terrorist activities in both countries. This convergent tendency can also be illustrated through reference to strategies on cyberterrorism from policy, legal and practical perspectives.

Firstly, in the policy dimension, according to the newly-published white paper and report from the SPC, the CCP emphasised ‘giving top priority to a preventive counterterrorism approach.’

Secondly, from the substantive law perspective, both jurisdictions have demonstrated a clear tendency toward the intensification of laws and punishments on terrorism. As previous chapters have shown, both jurisdictions have modified the existing laws and enacted new anti-terrorism laws which developed a pre-emptive framework to identify, manage and control the threats posed by terrorism.

Furthermore, through examining the existing anti-cyberterrorism legislation in both jurisdictions, it could be argued that both of them have taken an enhanced risk of paying less attention than necessary to basic criminal law principles. In particular, the following principles have often been ignored: certainty; proportionality; minimal

---

1316 See Chapter 5, section 5.3.
1317 See Chapter 7, section 7.2, 7.3.
criminalisation; and the presumption of innocence. These principles have been
developed in both examined jurisdictions to ensure that the criminal justice system
complies with the rule of law. In light of this, the counter-terrorism approaches must
strictly abide by these basic criminal law principles mentioned before. Otherwise,
excessive criminal measures would deviate from these basic principles and eventually
lead to the abuse and arbitrariness of state power.

Thirdly, from the practical perspective, both jurisdictions have introduced excessive
measures to fight terrorism (although specific legal regulations and practical
application are different in the respective jurisdictions). In addition, it has been
observed that in both countries, terrorism is used as a pretext to criminalise acts
actually unrelated or only remotely related to terrorism. Furthermore, anti-terrorism
laws tend to expand rather than diminish, and this expansion does not necessarily
correlate with the actual threat.\footnote{A Oehmichen, ‘Terrorism and anti-Terror Legislation—the Terrorised Legislator?: A Comparison of Counter-Terrorism Legislation and its implications on human rights in the legal systems of the UK, Spain, Germany, and France’ (DPhil thesis, Leiden University 2019) 310.}

The restrictive measures in the CTL in China are quite similar to the control orders,
TPIMs and other non-criminal methods of disruption in E&W, which focus on the
authorisation of pre-emptive discretion allowing the police to be proactive in response
to terrorism. For example, imposing restraints on individuals' freedom are
characteristic of many counter-terrorism operations in both jurisdictions, most notably
in the form of preventive detention and control orders. There is also a trend in both
jurisdictions to use administrative detention in response to preparatory cyberterrorist
acts. However, the practical flexibility of such administrative measures may cause
arbitrariness and abuses of power.

8.3.2 Broad and Vague Definition of Terrorism

Various observations emerged from the comparative analysis of the definitions of
terrorism in China and E&W.
There is no specific definition of cyberterrorism in both jurisdictions’ legislation, with both instead relying on the existing definition of terrorism as the legal foundation. According to critical analysis of the definition of terrorism in previous chapters, both jurisdictions have applied an overbroad and vague definition, which could violate legal certainty and clarity, resulting in arbitrariness.

The definitions of China and E&W appear to be quite similar in a number of important respects. Firstly, both include a ‘motive clause,’ an explicit reference to political, religious, racial or ideological purposes, as a basis for the commission of terrorist activities. Secondly, both definitions entail similarly broad terms of ‘violence or threat’ which implies that threats to use violence will also be classified as terrorism. In addition, the harm threshold is quite low and extensive in both cases, which is subject to criticism on account of lesser harms being considered worthy of criminal intervention. Thirdly, both have an intent requirement.

The definitions of terrorism in both jurisdictions are too broad and vague to violate the principle of certainty, which may categorise political dissenters as terrorists. Accordingly, in practice, relying on police and prosecutorial discretion to ensure appropriate application of the definition could resolve issues pertaining to its breadth and uncertainty. Such excessive reliance on discretion may undermine the rule of law and lead citizens to be unclear as to whether their acts are against the law or not.

In addition to the common points regarding definitions of terrorism analysed above, I argue that China’s definition is more expansive than that of E&W. Firstly, China’s definition of terrorism criminalises ‘proposition,’ which implies that ‘expression or speech’ related to terrorism may be subject to a terrorism designation. Secondly, the definition of ‘terrorism’ is often conflated with ‘separatism’ and ‘extremism’ which means that in the eyes of the CCP, both extremism and separatism fall under terrorism and should be combated similarly. Thirdly, China’s overbroad and vague definition may lead to an expanded interpretation, which could be used to suppress or capture all sorts of non-terrorist activities. Indeed, it could be argued that the rationale

---

1319 These three reasons could be found in Chapter 5, section 5.3.5.
underpinning this is authoritarian and driven by a legal system based on rule by law.

I conclude by arguing that, due to overbroad definitions, the scope of specific terrorism offences may also be wide. This wide-reaching definition serves to further extend the reach of the criminal law through establishing preventive offences to criminalise acts of non-terrorist or remote harm, which may also violate the principle of minimal criminalisation.

8.3.3 Criminalisation of A Wide Range of Terrorism Precursor Offences

As demonstrated in previous chapters, both China and E&W have criminalised a wide range of inchoate offences related to terrorism (also referred to as precursor offences), which could be committed online and/or offline. Correspondingly, some similarities in these offences with respect to substantive criminal law in both China and E&W could be observed. Specific examples are highlighted below:

- Intensification of the crackdown on association with or the mere membership of proscribed organisations (S 12 of the TA 2000; Art. 120 of the CL);
- Focus on suppressing financial assistance or other tangible support for terrorism (S 15 of the TA 2000; Art. 120a of the CL);
- Criminalisation of a wide range of preparatory acts (S 5 of the TA 2006; Art. 120b of the CL);
- Criminalisation of the publishing of statements likely to be understood as direct or indirect encouragement or other inducement to commit, prepare or instigate acts of terrorism (S 59 of the TA 2000; S 1 of the TA 2006; Art. 120c of the CL);
- Overbroad offence of collection information or possession of items for terrorism (S 57 and S 58 of the TA 2000; Art. 120f of the CL); and
- Combating extensive giving or receiving of training related to acts of terrorism.

This leads us to some conclusions regarding the commonalities in the characteristics of China and E&W's anti-terrorism legislation.

(1) Both China and E&W have a similar tendency of expanding terrorist offences. For
example, the imposition of criminal liability covering associative and facilitative terrorism-related offences also laterally reflects an expansion of the scope of criminal law as a whole. As Roach observed: ‘[m]any new terrorism offenses enacted after 9/11 pushed the envelope of inchoate liability and came dangerously close to creating status offenses, thought crimes, and guilt by association.’ Simester and Von Hirsch held that the creation of such a series of offences after 9/11 and 7/7 led to the expansion of the substantive scope of criminal law, which distorted its remit and confounded basic principles of criminalisation, not least the requirement of normative involvement by the accused in acts of the principal. Resorting to criminalisation has had the effect of radically enlarging the substantive scope of the criminal law.

(2) The imposition of criminal liability has been shifted to an earlier stage. For instance, these terrorism-related offences extend the scope of the attempted liability to the early stage of preparation, which runs counter to the long-standing principle of attempted liability. In E&W, the usual rules on attempted liability is limited to conduct ‘which is more than merely preparatory to the commission of the offence.’ Liability is extended to merely preparatory conduct, which is remote from the commission of the substantive act of terrorism. Unlike E&W, merely preparatory acts under the Chinese legislation are generally subject to criminal liability. This implies that engagement with any preparatory terrorist acts is prosecuted at a much earlier stage than offences of criminal attempt.

(3) Another special commonality in the anti-terror laws in the two jurisdictions is potential ignoring or restricting of general criminal law principles. First, the early intervention and extension of criminal liability in both jurisdictions violates the principle of minimal criminalisation. Offences mentioned above not only apply to acts that are remote from real harm than the inchoate offences, but also punish a wider range of participants (those who have not directly committed terrorist acts but have an

---

1323 According to Art. 22 of CL, the criminal liability for preparatory acts is the commission of a concrete preparatory act, regardless of whether there have been harmful consequences as a result.
associative role). It is arguable that the risk of expansion of the reach of criminal law and early intervention may loom over and discourage previously innocent interactions. In addition, both jurisdictions have taken a similar risk of 'criminalizing curiosity,' which means both extended their anti-terrorism laws to cover uploading or downloading terrorism-related materials without proving any specific intention.\textsuperscript{1324} By doing so, it may criminalise innocent curiosity and have a chilling effect on freedom of expression.

Second, the vagueness of these inchoate offences and the lack of clarity of specific terms in both jurisdictions violate the principle of legal certainty. For example, there are numerous vague and open-ended terrorism-related provisions, and also vague and uncertain criteria for measuring the severity of the circumstances in China.\textsuperscript{1325} In E&W, there are also many broad and uncertain terms (such as 'indirect encouragement,' 'collection information' and 'possession of items').

Third, the lack of proximity to the commission of the ultimate harm and the risk of harm and correspondingly harsh punishment may violate the principle of proportionality. For example, in China, the sentencing range for those who organise and lead a terrorist organisation was changed from 3-10 years to a mandatory minimum of 10 years.\textsuperscript{1326} In E&W, the maximum sentences available with respect to precursor crimes are high, despite the remoteness, the maximum penalty for preparatory offences is life imprisonment and many offenders have been handed lengthy sentences of 20 years or more.\textsuperscript{1327}

(4) A general shift to the prevention rather than repression can be observed. For substantive criminal law in both jurisdictions, the shift towards prevention is evidenced by the increasing tendency to establish a wide range of preparatory acts, incitement acts, fundraising acts or other remote acts, rather than harmful acts themselves (such as a terrorist attack). The motivation behind the emphasis on prevention is triggered by the great damage potentially brought by terrorism today. It is thus necessary to intervene in terrorist acts at an early stage to prevent harmful consequences from even

\textsuperscript{1324} See Chapter 5, section 5.3.4 and Chapter 7, section 7.3.2.8.
\textsuperscript{1325} See Chapter 5, section 5.4.1.
\textsuperscript{1326} See chapter 5, section 5.3.2.
\textsuperscript{1327} See chapter 7, section 7.7.
8.3.4 Broad Discretion of Executive Organs to Designate Proscribed Terrorist Organisations

<table>
<thead>
<tr>
<th></th>
<th>England &amp; Wales</th>
<th>China</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisions</td>
<td>S 3 of TA 2000</td>
<td>Art.120 of CL</td>
</tr>
<tr>
<td>Grounds for proscription</td>
<td>Any organisations “concerned in terrorism”</td>
<td>Failure to define what constitutes a “terrorist organization”</td>
</tr>
<tr>
<td>Designation authorities</td>
<td>• Secretary of State</td>
<td>• National Counter-Terrorism Leading Organ</td>
</tr>
<tr>
<td>De-proscription authorities</td>
<td>• Secretary of State</td>
<td>• National Counter-Terrorism Leading Organ</td>
</tr>
<tr>
<td></td>
<td>• Proscribed Organisations Appeal Committee</td>
<td>• The court</td>
</tr>
<tr>
<td>Similarities</td>
<td>Is the designation body the review body?</td>
<td>yes</td>
</tr>
<tr>
<td>Constitutional implications</td>
<td>• Separation of powers</td>
<td>• Judicial independence</td>
</tr>
</tbody>
</table>

Figure 8.1: comparison of designation procedures for proscribed terrorist organisations in China and E&W

According to this table, there appear to be some similarities between China and E&W related to the proscription of terrorist organisations. Firstly, both China and E&W have broad grounds to designate the proscription of terrorist organisations, which leaves the door open for the law to be deployed against any groups, organisations or religious associations that the state deems to be a threat whether they be political or non-political or non-violent. In addition, the broad definition of terrorism in both jurisdictions may also result in a degree of flexibility and arbitrariness for the executive branches in the designation of terrorist organisations and terrorists themselves. Secondly, both China and E&W mainly rely on administrative organs and grant them wide discretion to designate terrorist organisations. Thirdly, designation bodies are also review bodies in
both jurisdictions. The lack of successful de-proscription however implies that the executive itself is reluctant to de-proscribe.

8.3.5 Aggravated Punishment for Terrorism-related Offences

China and E&W appear to be prone to a similar tendency toward the intensification of laws and punishments in relation to terrorism during the post-9/11 era. More specifically, facing the increasing risk of domestic and international terrorism, both China and E&W have been gradually enacting stringent laws to control and punish terrorists. As shown in the analysis above, terrorism-related offences have become more preventive with sentences very strict indeed. For example, in China, the sentencing range for those who organise and lead a terrorist organisation was changed from 3-10 years to a mandatory minimum of 10 years.1328

Due to criminal law’s early intervention in most terrorism-related offences, and remoteness from the commission of a substantive act of terrorism, it is particularly difficult to achieve proportionality of punishment. In E&W, for example, offences of possession of proscribed materials, the dissemination of material that glorifies terrorism, and preparatory acts of terrorism all exist.1329 The maximum sentences available with respect to such crimes are high. For example, despite their remoteness, the maximum penalty for preparatory offences is life imprisonment and many offenders have been given lengthy sentences of 20 years or more.1330 Indeed, many offences carry a maximum sentence of life. In addition, the Counter-Terrorism Act 2008 s.30 contains provisions for ‘enhanced sentencing’ of offences with a ‘terrorist connection.’ According to this provision, ‘terrorist connection’ serves as an aggravating factor, which means subsequent terrorism-related offenders shall be given a draconian sentence. However, since ‘pretext’ offences may be imposed because of the difficulty to prove actual terrorism offences, it is doubtful whether there would be sufficient foundation for aggravating on the grounds of a terrorism connection.1331 The principle of proportionality requires that the severity of offences should be commensurate with the

---

1328 See chapter 5, section 5.3.2.
1329 See chapter 7, section 7.3.2.
1330 See Chapter 7, section 7.3.2.6.
severity of punishments for related crimes. In light of this, the problems of proportionality caused by pre-inchoate and associative liability and by the use of s.30 ‘terrorist connection’ charges are challenging. This is because it is doubtful whether the gravity of the act actually committed and the uncertain future harm are proportional to the severity of the punishment.

Similarly, in China, terrorism-related offences serve as an aggravating factor, which means re-offenders of terrorism-related offences shall be given a heavier punishment. The report of the SPC also showed that China has increased penalties for terrorism-related offences. Moreover, the maximum aggregate sentence for ringleaders or other principal leaders of terrorist organisations (who also commit murder, perform explosions, and engage in kidnapping) may ultimately be capital punishment.

In order to pursue proportionality of punishment, China has adopted the Balancing Leniency and Severity policy as a basic criminal justice policy, with sentencing for serious crimes carried out in a more nuanced manner. The shift from a ‘hard-strike campaign’ and ‘crackdown’ to ‘balancing leniency and severity’ indicates that the CCP adheres to the rule of law to combat terrorism to a certain extent.

8.3.6 Extension of Executive Powers

Both jurisdictions’ anti-terrorism legislation are increasingly focused on prevention rather than retribution. This means the vast majority of anti-terrorism laws have extended executive powers to interrogate, detain and control suspected terrorists during preliminary investigation or pre-charge periods. According to the analysis in the previous chapters, both China and E&W showed the following commonalities in their anti-terrorism enforcement measures:

- Expansion of the duration of detention;

---

1332 The details could be shown in Chapter 5, section 5.4.3.3.
1333 Ibid.
1334 See chapter 5, section 5.3.1.
1335 Ibid.
• Empowering executive organs with broad discretion to issue control orders and TPIMs;
• Erosion of presumption of innocence;
• Expansion of executive organs’ power in terrorism cases to investigate, detain and control suspects; and
• Similar tendency of using non-criminal disruption methods to deal with preparatory cyberterrorist acts.

(1) Expansion of the duration of detention

It could be observed that both jurisdictions have extended the period of pre-charge detention unanimously on the grounds of terrorism. In E&W, pre-charge detention under the TA 2000 was extended from 7-14 days to a maximum of 28 days under the TA 2006.\textsuperscript{1336} Furthermore, the TA 2008 extended the detention of terrorism-related suspects to 42 days. In China, according to Article 79 of the CPL, residential surveillance shall not exceed six months.\textsuperscript{1337} According to the CPL in China, the normal maximum period of pre-charge detention is two months, but under special circumstances this period can be extended repeatedly upon the approval of the procuratorate or the SCNPC for up to seven months.\textsuperscript{1338} This extended period is purportedly justified by the special difficulties in investigating such cases and the severity of the expected harm, but it deviates greatly from the normal maximum and causes an erosion of individual rights.\textsuperscript{1339}

(2) Empowering executive organs with broad discretion to issue control orders and TPIMs

Both China and E&W empowered their executive organs to use a control order regime in the course of investigating suspected terrorists.

\textsuperscript{1336} Under the Terrorism Act 2006, terrorist suspects could be held for up to 28 days. This statutory period lapsed in January 2012 with the result that the maximum term reverted to 14 days.
\textsuperscript{1337} CPL, Art.76.
In China, only the police (the head of public security organs) have the power to issue control orders, without the supervision of procuratorates and courts. In China, according to Article 53 of the CTL, police have great discretion to implement restraint measures against suspected terrorists, such as electronic surveillance and irregular inspection.

In E&W, the executive organs (the police and Home Secretary) are given the power to prevent terrorists from carrying out terrorist acts. The enforcement measures to prevent terrorism mainly include: (1) under s 44 of the TA 2000, the police were empowered to stop and search any vehicle or person in certain areas within their jurisdiction without any suspicion that the vehicle/person may be connected with terrorism; (2) the Home Secretary being empowered with the discretion to impose obligations on suspected terrorists under the control order system under s 1 of the PTA 2005; and (3) the control order regime, which was then replaced by TPIMs, which was also issued by the Home Secretary. The obligations which could be included in a control order were similar to those in the Chinese regime, including restrictions on movement and association with certain persons, wearing an electronic tracking device, telecommunications, and the use of the Internet.\(^\text{1340}\)

\section*{(3) Erosion of the presumption of innocence}

In order to pursue prevention of future harm, police and the prosecution services intervene prior to the commission of harmful acts in both jurisdictions. The focus on prevention leads to a risk of criminalising innocent people, which erodes the presumption of innocence.

In E&W, facilitating the successful prosecution of suspected terrorists results in the erosion of their procedural protection in the criminal process. As Ashworth observed: ‘there is evidence that the criminal justice model is being stretched and, possibly, over-extended by the invocation of preventative rationales.’\(^\text{1341}\) Taking the possession

\(^{\text{1340}}\) Prevention of Terrorism Act 2005, s 1(4).

offence as an example, the reverse burden of proof may violate the presumption of innocence\textsuperscript{1342} because the article possessed will often be lawful and might have many uses\textsuperscript{1343} with regard to judicial interpretation.

In China, these issues runs deeper, whereby as long as the offender commits terrorism-related acts (e.g. holding terrorism-related materials, or downloading or uploading violent terrorism videos), they will be punished under the CL or the CTL, regardless of whether or not they have a specifically terrorist intention. In judicial practice, even if the accused proves that they are simply acting in curiosity, they are still convicted, obviously eroding the presumption of innocence principle.\textsuperscript{1344}

(4) Expansion of executive organs’ power in terrorism-related cases to investigate, detain and control suspects

Both China and E&W grant the executive organs wide discretion to investigate, detain and control suspected terrorists for the purpose of preventing terrorism risks.

In China, the powers of the police have been continuously expanded to control suspected terrorists, and a series of obligations are given to these suspects to disrupt future threats through ‘secret detention’ of suspects,\textsuperscript{1345} residential surveillance (essentially house arrest),\textsuperscript{1346} implementing electronic surveillance, irregular inspections and other means of surveillance during the investigation as well as monitoring the communication of suspects.\textsuperscript{1347} All of these restrictions are broad and vague, raising doubts about legality and compatibility with the rule of law,\textsuperscript{1348} and

\textsuperscript{1343} Walker cites the examples of ‘wires, batteries, rubber gloves, scales, electronic timers, overalls, balaclavas, agricultural fertilizer, and gas cylinders’. C Walker, Blackstone’s guide to the anti-terrorism legislation (Oxford University Press 2009) 187.
\textsuperscript{1344} See Chapter 5, section 5.3.4.
\textsuperscript{1345} Art. 83 of the 2012 Criminal Procedure Law provides: After being taken into custody.. .the family members of the detained person should be informed within 24 hours, except for situations in which it is impossible to issue a notice or the detained person is suspected of com- mitting crimes endangering state security or crimes of terrorism and family notification may impede the investigation.
\textsuperscript{1346} According to Article 73 of CPL, the police are granted the discretion to place a suspect under residential surveillance at a designated location other than his/her domicile if residential surveillance at the suspect's domicile may impede the investigation of cases connected with terrorism.
\textsuperscript{1347} The details could be found in Chapter 5.
leaving considerable space for authorities' overuse of their detention powers.

Similarly, in E&W, the police maintain a pre-emptive function to prevent terrorists from carrying out terrorist acts.\cite{1349} For instance, under s 44 of the TA 2000, the police are preventively involved in stopping, questioning and searching suspects who pose a terrorist threat.\cite{1350} The police were also empowered with wider discretion to gather evidence and intelligence to support the criminal process such as with regard to detaining or releasing a suspected terrorist.\cite{1351} Meanwhile, s 1(4) of the PTA 2005 lists a lengthy catalogue of restrictions on personal freedom, including restrictions on movement, access and communication.\cite{1352} Non-derogating control orders are widely applied, including house arrest, curfew, electronic tagging, restricting the use of communication devices (such as a computer, phone or Internet), restricting access to others and travel bans.\cite{1353} Elsewhere, according to schedule 1 of the Act, the TPIM notice may contain any of the 12 types of measure, which are deemed necessary to prevent or restrict the individual’s involvement in terrorism-related activity, such as an overnight detention measure, an exclusion and/or movement directions measure and an electronic communication device measure.\cite{1354}

(5) Similar tendency of using non-criminal disruption methods to deal with preparatory cyberterrorist acts

Both China and E&W have a similar tendency when it comes to the use of non-criminal disruption methods to combat preparatory cyberterrorist acts for the purpose of prevention.

\textsuperscript{1349} The details could be found in Chapter 7.
\textsuperscript{1351} Especially following the London bombing in 2005, an unpopular side effect in the use of this power was the majority of citizens stopped by the police were disproportionately of black or Asian ethnicity. See A Parmer, ‘Stop and Search in London: Counter-Terrorist or Counter-Productive?’ (2011) 21(4)PS 369, 370.
\textsuperscript{1352} PTA 2005, s 1(4).
\textsuperscript{1353} PTA 2005, s 9.
\textsuperscript{1354} Ibid, s 3(4). The other eight types of measure are: travel measure; financial services measure; property measure; association measure; work or studies measure; reporting measure; photography measure; and, monitoring measure.
In E&W, non-criminal disruption methods are applied to suspected terrorists who cannot be prosecuted. Some reasons why these suspects involved in terrorist activities cannot be prosecuted are as follows: insufficient evidence (especially given that the intercept evidence cannot be used in criminal trials\(^\text{1355}\)); incriminating evidence cannot be disclosed on grounds of the public interest (e.g. to retain the cover and ensure the safety of human agents); and/or the individual has already served their sentence but is still assessed as a threat to national security.\(^\text{1356}\) Pertinently, Independent Reviewer Macdonald argued that TPIMs were created to re-align with the criminal justice system aiming to facilitate the prosecution, conviction and punishment of terrorists.\(^\text{1357}\) In this regard, this measure is an alternative to criminal justice for those who cannot be prosecuted but carry a threat to national security. In this situation, there is a tendency to use non-criminal disruption methods to deal with preparatory cyberterrorist acts for prevention purposes.\(^\text{1358}\)

In China, the tendency of using administrative detention to tackle preparatory terrorist offences has become more prominent. The Chinese authorities tend to apply administrative detention and restraint measures as an efficient and cost-effective approach to policing low-level offences.\(^\text{1359}\) This is because the police are granted broad discretion to detain and investigate suspected terrorists. The use of flexible police enforcement power is a popular crime control tool in contemporary China, but it may lead to abuses of power.

### 8.4 Conclusion

This chapter has argued that a state’s legal responses to cyber-terrorism is contingent on the nature of that state’s legal system. First of all, due to the huge differences between their legal and political systems, there are a series of differences in the

---

\(^{1355}\) Home Office, *Intercept as Evidence* (Cm 8989, 2014).
\(^{1358}\) The CONTEST advocates the use of other methods of disruption that sit outside the criminal justice process.
approaches of China and E&W to combat cyberterrorism. These differences mainly entail: (1) different judicial review process; (2) different legislative scrutiny and independent review systems; (3) different protections of suspected terrorists’ rights; and (4) different levels of human rights protection. All of these divergences are attributable to the different political and legal systems of the two jurisdictions (i.e. rule of law vs. rule by law, separation of powers vs. concentration of powers, human rights protection vs. national security, and independent judiciary vs. lack of judicial review).

However, there are many ways in which their legal responses converge, regardless of the differences in the nature of their legal systems. I argue that the legal responses in these two jurisdictions share the following similarities: (1) preventive and pre-emptive tendency to address cyberterrorism problems; (2) overbroad and vague definition of terrorism; (3) overcriminalisation of terrorism precursor offences; (4) broad discretion of executive departments to designate proscription; (5) aggravated punishment for terrorism-related offences; and (6) extension of executive powers. Therefore, in sum, differences in their legal systems do not explain the similarities in their legal responses particularly to cyberterrorism.

Therefore, if both rule by law and rule of law systems are capable of producing arbitrary, uncertain and disproportionate legal responses to ill-defined problems of cyberterrorism, then of the connection between such systems and corresponding responses is not necessary. Therefore, establishing what does have a necessary link with the production of such responses (e.g. hyperconnectivity threats that are so catastrophic they ‘necessitate’ pre-emptive or ‘precautionary’ legal responses jeopardising, in turn, the retrospective establishment of guilt beyond all reasonable doubt, on the facts and after the facts, all of which is central to due process in the rule of law) becomes a key question for further research in this field. All of these aspects will be elaborated upon in the conclusion chapter below.
Chapter 9 Conclusion

9.1 Introduction

This thesis has compared the relationships between legal regimes and legal responses to cyberterrorism in China and E&W to determine whether these relationships are necessary or contingent on other factors. It is unsurprising to find that there are many fundamental differences in the legal responses to cyberterrorism between China and E&W, which are attributable to the differences in legal and political systems in the two jurisdictions.\(^{1360}\) However, upon closer analysis, there are a number of key similarities in their approaches as well, suggesting that the nature of the legal system does not directly determine a jurisdiction’s legal responses to cyberterrorism.\(^{1361}\)

In light of this finding, the following question arises: what can explain the convergence of legal responses to cyberterrorism in these different jurisdictions? In this chapter, I put forward a few conjectures which might explain the similarities and differences identified and also suggest an agenda for further research. Furthermore, another implication of this thesis is the need for international cooperation to combat cyberterrorism. At present, there is lack of a special anti-cyberterrorism convention, so it is necessary to establish an international legal framework, reach international consensus and make global joint efforts to criminalize various forms of terrorist acts and exercise universal jurisdiction. There are some existing multilateral international or regional cooperation that can be used to combat cyberterrorism, such as the UN, Interpol and International Multilateral Partnership against Cyber Threats (IMPACT), etc.

9.2 Conjectures about the Convergence in Legal Responses to Cyberterrorism in China and E&W

Findings from the comparison of the legal responses of China and E&W to cyberterrorism suggest some degree of convergence in the following regards: in supra-

\(^{1360}\) See Chapter 8, Section 8.2.
\(^{1361}\) See Chapter 8, Section 8.2.
national demands for the harmonisation of counter-terrorism law to address cross-
national issues; the promotion of international cooperation; and the transfer of anti-
terrorism law and policy between different jurisdictions. In addition, the
interdependence of the global economy and related policy shifts are factors influencing
the convergence of legal responses to cyberterrorism.\footnote{278}

\textbf{9.2.1 Supra-national Demands for the Harmonisation of Counter-terrorism Law}

One area on which different jurisdictions’ anti-terrorism laws tend to converge is the
strong demand of supra-national institutions for harmonising anti-terrorism laws to
combat transnational terrorism.

As previous chapters have shown, in examining domestic anti-terrorism laws in China
and E&W, they are all affected to some extent by international anti-terrorism laws and
institutions. Reuven Young advanced the proposition that for legal and pragmatic
reasons, states should learn from the core elements of the international definition of
terrorism when developing their own domestic legal definitions.\footnote{90} In addition,
immediately after 9/11, the UN Security Council issued Resolution 1373, requiring
member states to ensure that terrorism and terrorist financing were considered serious
crimes in their domestic laws, without providing detailed guidance.\footnote{91} Meanwhile, the
Counter-Terrorism Committee was established to monitor compliance with these
resolutions by member states and to provide technical assistance in implementing
them.\footnote{92}

Although Resolution 1373 has been criticised for exceeding the authority of the

\footnote{278}{D Brewster, ‘Crime Control in Japan: Exceptional, Convergent or What Else?’ (2020) 60 (6)BJC
1547, 1566.}
\footnote{90}{R Young, ‘Defining Terrorism: The Evolution of Terrorism as a Legal Concept in International Law
and Its Influence on Definitions in Domestic Legislation’ (2006) 29(1) BCICLR23, 23-106.}
\footnote{91}{UNSC, Res 1373(28 Sep 2001) UN Doc S/RES/1373. Invoking mandatory language, the Security
Council ‘decided’ ‘that all States shall ... [c]riminalize the wilful provision or collection, by any means,
directly or indirectly, of funds by their nationals or in their territories with the intention that the funds
should be used, or in the knowledge that they are to be used, in order to carry out terrorist acts’ and
‘[e]nsure that ... the financing, planning, preparation or perpetration of terrorist acts ... are established as
serious criminal offences in domestic laws and regulations and that the punishment duly respects the
seriousness of such terrorist acts’.}
\footnote{92}{CH Powell, ‘The Role and Limits of Global Administrative Law in the Security Council’s Anti-
terrorism Programme’ in H Corder and J Bleazard (ed), \textit{Global Administrative Law: Innovation and
Developments} (Acta Juridica 2009) 32–67.}
Security Council and has even been considered ‘anti-constitutional,’\textsuperscript{1366} the Security Council issued a strikingly similar vague and broad resolution (Resolution 2178) in September 2014, requiring member states to further ensure that a series of precursor terrorism-related offences were considered serious crimes.\textsuperscript{1367} Similar to Resolution 1373, Resolution 2178 set off another round of expansion of terrorism offences even though it did not offer any guidance on the definition and scope of terrorism either, which may have led to the broadening of the term to encompass ‘violent extremism’ and ‘radicalization...which can be conducive to terrorism.’\textsuperscript{1368} Meanwhile, UN Security Council Resolution 1624 called on countries to criminalise incitement to terrorist acts\textsuperscript{1369}, as exemplified in the comparison of China and E&W in this thesis.\textsuperscript{1370}

In response to these UN resolutions, both China and E&W criminalised a wide range of terrorism-related precursor offences, which also apply to acts of cyberterrorism.\textsuperscript{1371} Resolution 1373 and its successors have created a legal template, which gives some guidance to various states’ anti-terrorism laws \textsuperscript{1372} and there is widespread coordination among governments on the implementation of these laws and the establishment of legal norms. Through these resolutions, the Security Council is recognised as playing the role of international legislator \textsuperscript{1373} and has assumed the power to monitor the compliance of domestic legislation with international law.\textsuperscript{1374} As such, the Security Council plays an important role in the globalisation of the legal framework for counter-terrorism.\textsuperscript{1375} Roach argued that E&W's anti-terrorism laws

---


\textsuperscript{1367} UNSC, Res 2178(24 Sep 2014) UN Doc S/Res/2178, para 6. It requires all states to ensure that travel to plan, prepare, provide or receive terrorist training, or participate in or perpetuate terrorist acts be treated as serious criminal offences. UNSC, Res 2178(24 Sep 2014) UN Doc S/Res/2178, para 6.


\textsuperscript{1370} Such as the UK and China, the details could be found in Chapter 5 and 7.

have served as templates for global migration.\textsuperscript{1376} This raises an important line of inquiry for further research: which legal responses to global threats, such as cyberterrorism, and from which particular states are being generalised by key international legislators, such as the UN Security Council? In turn, what resistance, if any, is there from other states who are becoming ‘net importers’ of legal responses originating in other nation-states? Consequently, how might this strategic relationship between the power of ‘net exporters’ of legal responses and the resistance from net importers help us to explain the propagation of international legal responses to transnational threats? In addition, how does this relationship help us explain the convergences and differences in legal approaches between different jurisdictions in response to the same transnational threat?

In addition to UN resolutions, regional anti-terrorism legal frameworks (such as the EU Guideline Decisions on terrorism laws) are also an important supra-national driving force when it comes to enacting domestic anti-terrorism legislations.\textsuperscript{1377} In view of this, I envision that these supra-national anti-terrorism legal frameworks are considerable contributors to the convergence of domestic anti-terrorism laws (including those of China and E&W), which would be at the extreme satisfied by a uniform and homogeneous global counter-terrorism law. Meanwhile, again, an important avenue for further research will be understanding how resistance to net exporters of international law shapes the actual propagation of legal responses to global threats across different legal systems.

9.2.2 Demanding the Promotion of International Cooperation


The second conjecture regarding the convergence of anti-terrorism laws between different jurisdictions is the perceived need for international cooperation to deal with transnational terrorism. The transnational threat of cyberterrorism has also increased the need for different degrees of international cooperation and coordination between countries.\textsuperscript{1378} For instance, the UNSCR 1373 required the promotion of international cooperation and implementation of the then 12 terrorism-related multilateral treaties.\textsuperscript{1379} It also called on countries to assist each other by exchanging information and 'cooperating in administrative and judicial matters to prevent the commission of terrorist acts.'\textsuperscript{1380} In counter-terrorism practice, cooperation and coordination between governments of various countries have been continuously strengthened, especially the information-sharing of intelligence agencies on national security affairs.\textsuperscript{1381}

In addition, convergence also depends on the uncertainty of terrorism, as well as the degree of inter-organisational dependency and professional communication.\textsuperscript{1382} Some scholars believe that transnational cooperation and the gradual establishment of a more complete and interdependent world order are powerful determinants of policy convergence.\textsuperscript{1383} According to policy convergence theory, recognising a common problem and establishing institutions to combat it increases the possibility that national policies will become more similar over time.\textsuperscript{1384} It could be observed here that anti-

\textsuperscript{1378} Two illustrative examples involve the appointment of an EU counterterrorism coordinator and the establishment of Eurojust to enhance coordination of investigations and prosecutions related to terrorist crimes. Other interorganizational bodies (Europol, the Berne group, the Counterterrorist Group) aim at facilitating cooperation between member states.


terrorism efforts within an international or regional framework (such as the UN, the EU or other international organs) will promote the gradual convergence of national anti-terrorism policies.\footnote{D Nohrstedt and D Hansén, ‘Converging Under Pressure? Counterterrorism Policy Developments in the European Union Member States’ (Public administration, Feb 2010)\textit{https://doi.org/abc.cardiff.ac.uk/10.1111/j.1467-9299.2009.01795.x} assessed 31st July 2020.} The theory of convergence also emphasises the influence of intergovernmental organisations and supra-national laws on domestic anti-terrorism law and policy-making.\footnote{The promotion of international partnership constitutes one important dimension of the EU’s work on counterterrorism, as expressed by the EU counterterrorism strategy, Council of the European Union, ‘The European Union Counterterrorism Strategy’ (European Council, 2005)\textit{https://www.consilium.europa.eu/en/policies/fight-against-terrorism/eu-strategy/} accessed 20 Aug 2020; S Bulmer and S Padgett, ‘Policy Transfer in the European Union: An Institutionalist Perspective’ (2004) 35BJPS 103, 103–126. K Roach, ‘A Comparison Australian and Canadian Anti-terrorism laws’ (Research gate, January 2007) \textit{https://www.researchgate.net/publication/228162190} accessed 28 September 2020.} Again, however, an important avenue for further research is to understand resistance to, and the exercise of political power in the competition over, the putative influence of intergovernmental organisations.

9.2.3 The Transfer of Anti-terrorism Law and Policy between Different Jurisdictions

The third conjecture about tendencies toward the convergence of legal approaches to terrorism between different jurisdictions is the transfer or transplantation of anti-terrorism laws and policies. Globally, anti-terrorism laws converge on two dimensions: at the horizontal level, they converge in principle and practice through coordination and borrowing between countries; and, at the vertical level, they converge through the adoption of international anti-terrorism legal norms and standards. The emergence of more and more counter-terrorism laws shows that counter-terrorism measures are moving in the direction of transnational transfer, and such transfer works at both an international and a domestic level.\footnote{LK Donohue and J Kayyem, ‘Federalism and the Battle over Counter-terrorist Law: State Sovereignty, Criminal Law Enforcement, and National Security’ (2002) 25 SCT1, 1.} This demonstrates that whereas international legislators, such as the UN Security Council, drive convergence in legal responses through the ‘top-down’ imposition of legal norms, convergence can also occur from the ‘bottom-up’ as legal norms are transferred through bilateral, or even multilateral, relations between particular states who seek to import from elsewhere those legal
responses which they perceive to be ‘best practice.’

A hyperconnected world enables people to communicate and interact with others anytime and anywhere, while more and more things are now connected. Such hyper-connection enhances the spatial coverage and therefore the risks of cyberterrorism. Fighting against cyberterrorism is becoming a preoccupation of an ever-widening circle of nations due to the threat it poses to a wide range of jurisdictions. In the era of globalisation, combating the transnational issue of cyberterrorism entails the interaction of international, regional and domestic anti-terrorism policies and laws. In this vein, countries or jurisdictions may seek a comprehensive solution, which usually reflects the integration of the civil law and the common law components, and which may involve the transfer of anti-terrorism laws and policies. Again, however, such convergence is only liable to be reproduced where ‘comprehensive’ or ‘universal’ solutions are in alignment with the changing strategic interests of nation-states. So, another key avenue for further research is to investigate the impact of conflicting strategic interests with respect to the international propagation of legal responses to global threats.

Traditionally, international comparative law promotes legal transplantation, which is reflected in the trend of relevant countries to adopt similar measures; countries with more sophisticated legal systems have a greater impact on developing countries.

---


1391 KL Scheppele, ‘International standardization of national security law’ (2010) 4(2) JNSLP 438; M Graziaide, ‘Comparative law as the study of transplants and receptions’ in M Reimann and R Zimmermann (eds) Oxford Handbook of Comparative Law (Oxford University Press 2006) 441; W Osiatynski, Paradoxes of Constitutional Borrowing’ (2003) 1(2) IJCL 244, 244-266; S Choudry (ed), e
The same is true for the transplantation of anti-terrorism laws. Many countries have set their sights on other countries when drafting or implementing anti-terrorism laws, which has led to horizontal convergence. For instance, after 9/11, a profusion of national anti-terrorism legislation emerged, which saw the adoption of the UK’s Terrorism Act 2000 and the US’s Patriot Act 2001 for instance. In particular, the UK’s anti-terrorism laws have had a significant impact on other countries (including Australia, Canada, Malaysia, Singapore, Ethiopia and India). Such policy transfer may be motivated by an admiration for the content and design of counter-terrorism laws in developed countries, or suggestions from international institutions such as the UN’s Counter-Terrorism Committee or the Financial Action Task Force (FATF). For example, some international organisations, such as the United Nations Office on Drugs and Crime (UNODC), are committed to the transmission and harmonisation of anti-terrorism laws through model legislation on anti-terrorism financing.

International organisations are playing an increasingly mandatory role in requiring countries to adopt certain types of anti-terrorism regulations. For instance, Resolution 1373 requires member countries to formulate new criminal provisions against terrorist

---


1396 Other examples in the anti-terrorism financing area include the UN Office on Drugs and Crime’s model legislation on money laundering and terrorism financing <www.unodc.org/unodc/en/money-laundering/Model-Legislation.html> and the work of the Financial Action Task force (FATF).
financing, to freeze the assets of individuals and organisations related to terrorism, and
to prevent contributions to terrorist organisations.\textsuperscript{1397} The United Nations is not the
only agency to take coercive action to ensure the transnational transplantation of anti-
terrorism laws. For example, the FATF is ‘an inter-governmental body whose purpose
is the development and promotion of national and international policies to combat
money laundering and terrorist financing.’\textsuperscript{1398}

\section*{9.3 Conjectures Explaining Divergence in Legal Responses to Cyber-
terrorism in China and E&W}

Due to difference in jurisdictions' political and legal systems, their legislative
frameworks and implementation of laws in response to cyberterrorism will inevitably
have many differences. For example, the independent judicial review and legislative
review systems of China and E&W are notably different, resulting in divergences in
their response to cyberterrorism and their implementation of cyberterrorism laws (such
as safeguarding suspected terrorists’ rights, the review of permissions for control
orders, and the review of administrative power abuse).\textsuperscript{1399} The differences here shows
that a jurisdiction’s laws and practices against cyberterrorism are essentially rooted in
their unique legal, political, cultural and social background.\textsuperscript{1400}

Furthermore, as mentioned in the analysis above, although domestic anti-terrorism
laws are affected by the international legal framework and the anti-terrorism laws of
the UK and the US, national security and sovereignty are barriers to the convergence
of anti-terrorism legal approaches\textsuperscript{1401}, as well as within nation-states amongst
competing regional powers. This raises the question of how the exercise of political
power in the competition amongst rival, multiple centres of governance shapes

\begin{footnotesize}
\textsuperscript{1397} CH Powell, ‘The United Nations Security Council, Terrorism and Rule of Law’ in V Ramraj and
others(ed), \textit{Global Anti-Terrorism Law and Policy} (2nd ed, Cambridge University 2012) 19-43; See also
V Ramraj, ‘The impossibility of anti-terrorism law?’ in V Ramraj and others(ed), \textit{Global Anti-Terrorism
1.
\textsuperscript{1399} The details could be found in Chapter 8.
\textsuperscript{1400} H Lu, B Liang and M Taylor, ‘A Comparative Analysis of Cybercrimes and Governmental Law
\textsuperscript{1401} Daniel Alati, ‘Domestic Counter-terrorism in a Global Context: A Comparison of Legal and Political
Structures and Cultures in Canada and the United Kingdom’s Counter-terrorism Policy-Making’(DPhil
\end{footnotesize}
responses to security threats, including the bargaining and negotiation of various power-dependencies. Accordingly, this strategic and relational concept of political power implies the need for further research into how sovereign states respond to resistance to the exercise of their power, which happens within as well as between nation states and their claimed jurisdictions of sovereign writ.  

In addition, domestic structures and cultures, including the legal system, the relative stability of government, local human rights culture, and geopolitical relationships all also have significant impacts on the evolution of counter-terrorism policies in different jurisdictions. 

Besides, legal transplantation is jointly promoted by internal and external pressures. Internal pressures, including the growing threat of domestic terrorism, have led people to seek "foreign" solutions to similar problems; external pressures require countries to seek common solutions to deal with the urgent international terrorism problem. However, some comparative law scholars are increasingly suspicious of the effects of ‘transplanting’ processes and procedures from one national and legal culture into another. Some legal transplants may not achieve the expected results, for example where the internal institutions and cultural resistance of the receiving system are too strong. As noted by Ramraj, although this coercive mechanism is powerful, the practical consequences after the transplantation of anti-terrorism law are not completely consistent. Part of the challenge here derives from the formal differences between legal systems; partly from the unique political, historical, 

\[1402\] A Edwards, ‘Multi-centred governance and circuits of power in liberal modes of security’ (2016) 17(3-4)GC 240,240-263. 
\[1403\] Ibid. In its analysis of security certificates and bail with recognizance/investigative hearings in Canada, and detention without trial, control orders and TPIMs in the UK, this thesis reveals how domestic structures and cultures, including the legal system, the relative stability of government, local human rights culture, and geopolitical relationships all influence how counter-terrorism measures evolve. 
\[1405\] Particularly since 9/11, however, a tension has opened up between those who would seek to deal with the problems of international terrorism through war and those who would seek to deal with it through international cooperation and law which makes the search for common legal solutions among the latter all the more urgent. See PB Heymann, Terrorism, Freedom and Security (MIT Press 2003). 
cultural, and socio-economic conditions of each jurisdiction, and partly from the uncertainty and vagueness inherent in the concept of terrorism.\textsuperscript{1408} I argue that this factor could well explain the differences in the legal responses to cyberterrorism between different jurisdictions.

The comparative study of domestic anti-terrorism laws could provide for a better understanding of convergences and divergences in the legal approaches to terrorism in different jurisdictions, and may also explain how these states cater to the strong supra-national demands for the harmonisation of law. As mentioned earlier, supra-national bodies (such as the UN and the EU) are committed to encouraging member states to enact domestic anti-terrorism laws and, through critical inspections, there is a tendency to broadly define and expand the scope of terrorism offences. But, interestingly, although the anti-terrorism laws in various states are similar in wording, there are huge differences in the 'law in action' of such approaches due to their different political, legal and cultural systems\textsuperscript{1409}, and also because of conflicting interests and thus strategic relations of power. What is surely needed in any future research agenda on the dynamics of convergence and divergence in legal responses to global threats is an understanding of these strategic relations and the political competition to govern generated by these relations.

\section*{9.4 International Cooperation against Cyberterrorism}

Another implication of this thesis is the need for international cooperation to combat cyberterrorism.\textsuperscript{1410} For example, the International Atomic Energy Agency proposed “the need for a legal framework (incorporating international treaties and agreements) to develop measures for jurisdictional prosecution and cross-border enforcement”.\textsuperscript{1411}

\begin{itemize}
\item \textsuperscript{1408} Ibid.
\item \textsuperscript{1409} A few countries such as Brazil have so far resisted supranational pressures to enact terrorism laws. RS Costa, ‘Brazil’ in K Roach(ed), \textit{Comparative Counter-Terrorism Law} (Cambridge University 2015) 148.
\item \textsuperscript{1410} M Dogrul, A Aslan, E Celik, ‘Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism’ (3rd International Conference on Cyber Conflict, Estonia, 2011) 1; K Prasad, ‘Cyberterrorism: Addressing the Challenges for Establishing an International Legal Framework’ (3rd Australian Counter Terrorism Conference, Perth, 3\textsuperscript{rd} –5\textsuperscript{th} December 2012) 10.
At present, there is lack of a special anti-cyberterrorism convention, so it is necessary to establish an international legal framework, reach international consensus and make global joint efforts to criminalize various forms of terrorist acts and exercise universal jurisdiction.\textsuperscript{1412} Moreover, the lack of a special convention against cyberterrorism has prompted multilateral international organizations to enhance security through harmonisation of legislation, coordination and cooperation in law enforcement and utilisation of anti-cyberterrorism actions.\textsuperscript{1413} Due to the transnational nature of cyberterrorism, it is necessary to coordinate legislation to prevent cyber terrorists from taking advantage of judicial and legal loopholes between countries and prevent them from carrying out cyberterrorism activities.

Additionally, Lewis claimed that international cooperation is the key means to establish cyber security. Similarly, Pardis \textit{et al.} argued that since regional and bilateral agreements and local legislation are insufficient to deter cyberterrorism, international law is a necessary tool to enable the international community to curb cyber threats within its different jurisdictions.\textsuperscript{1414} Goodman and Brenner argued that cyberterrorism requires an international legal framework to deal with, so countries must strengthen cooperation and introduce a series of consensus on core terrorist crimes, which can be applied against cyber criminals in any jurisdiction.\textsuperscript{1415} Similarly, Cassim claimed that the fight against cyberterrorism is not only through the formulation of strict legislation and strengthening cyber security measures, but also through international cooperation.\textsuperscript{1416} Although States must also enact legislative measures to combat cyberterrorism and other misuse of technology, such mechanisms also need appropriate support from international agreements.\textsuperscript{1417} Krishna Prasad put forward

\begin{itemize}
\item \textsuperscript{1412} K Prasad, ‘Cyberterrorism: Addressing the Challenges for Establishing an International Legal Framework’ (3rd Australian Counter Terrorism Conference, Perth, 3\textsuperscript{rd} -5\textsuperscript{th} December 2012) 12.
\item \textsuperscript{1413} PM Tehrani, NA Manap and H Tajli, ‘Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime’ (2013) 29 CLSR 207, 215.
\item \textsuperscript{1414} PM Tehrani, NA Manap and H Tajli, ‘Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime’ (2013) 29 CLSR 207, 207.
\item \textsuperscript{1415} MD Goodman and SW Brenner, ‘The emerging consensus on criminal conduct in cyberspace’ (2002) 10(2) JTLIT 139, 223.
\item \textsuperscript{1416} F Cassim, ‘Addressing the spectre of cyber terrorism: A comparative perspective’ (2012) 15(2) PELJ 381, 405.
\item \textsuperscript{1417} L Bantekas, \textit{International Criminal Law} (3rd edn, Routledge-Cavendish Publication 2007) 265.
\end{itemize}
four key critical elements for establishing an effective international legal framework: “agreement on the definition of cyberterrorism; leadership by the United Nations (UN); utilization and expansion of existing international conventions, legislation and authorities to create a cohesive and robust system; and effective law enforcement.”1418

At present, there are some existing multilateral international or regional cooperation that can be used to combat cyberterrorism.

1. United Nations (UN)

The UN is an international organization that leads member states in coordinating and cooperating in combating international terrorism.1419 For example, a series of UN resolutions are committed to combating different types of terrorism: Resolutions 55/63 (2000)1420 and 56/121 (2001)1421 on Combating the Criminal Misuse of Information Technology, Resolution 1624 (2005)1422 and Resolution 1617 (2005).1423 Additionally, Resolution 1535 established the Counter-Terrorism Committee Executive Directorate (CTED) which promotes cooperation among member states and regional and inter-government agencies and provides technical assistance.1424 Specially, the UN General Assembly adopted Resolution A/RES/2321 on cyberterrorism in 2008 and a resolution on the “creation of a global culture of cyber security and taking stock of national efforts to protect critical information infrastructures” in 2010 which calls on member states to share measures to protect cyber security and critical infrastructure.1425 Considering that it takes a long time to formulate a treaty and the lack of comprehensive international legal documents against cyberterrorism, the UN resolution is an effective and realistic method to deal with cyberterrorism at present.1426

1418 Ibid.
1420 UN General Assembly, Resolution 55/63 (4 Dec 2000), UN Doc A/RES/55/63.
1421 UN General Assembly, Resolution 56/121 (19 Dec 2001), UN Doc A/RES/56/121.
1422 UN Security Council, Resolution 1624 (14 Sep 2005), UN Doc S/RES/1624.
1426 J Trahan, ‘Terrorism Convention: Existing Gaps and Different Approached’ (2002) 8(2) NEJICL 215, 221-222; YN Ong, ‘International Responses to Terrorism: The Limits and Possibilities of Legal Control of
In addition, Pardis et al. proposed that existing international law which is designed to tackle terrorism could and should be adapted to address cyberterrorism, which could be modified to deal with rapidly changing technologies and to cover new situations.\(^{1427}\) Therefore, most international anti-terrorism treaties or legal documents can be applied to cyber terrorism. For example, now there has been established 17 specific conventions (including its complimentary) and major legal instruments which deal with terrorist activities and which may be applicable to cyberterrorism.\(^{1428}\)

Furthermore, although the UN has also issued a number of resolutions to combat terrorism, a unified definition of terrorism has not yet been formulated. It has been criticized that the failure of the UN to formulate legal instruments because it focuses too much on reaching consensus on existing methods that terrorists have used, so it is unable to lead the fight against new methods, such as cyberterrorism.\(^{1429}\) Therefore, drawing on the experience of the UN, international legal framework should avoid overly reactive (rather than proactive) to deal with the threat of cyberterrorism.\(^{1430}\)

2. Interpol

In response to the rapid increase in international terrorist attacks, Interpol established a counter-terrorism section in September 2002, called the Fusion Task Force (FTF). Its main purpose is to provide information about terrorist organizations and their membership, collect and share intelligence, improve member states' anti-terrorism capabilities, and provide technical support.\(^{1431}\) Interpol has established a priority to combat crimes related to public safety and terrorism, and uses its special status in

\(^{1427}\) PM Tehrani, NA Manap and H Taji, ‘Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime’ (2013) 29 CLSR 207, 211.


\(^{1430}\) Ibid.

international law enforcement to assist countries in combating terrorism.\(^{1432}\)

3. International Multilateral Partnership against Cyber Threats (IMPACT)

The International Multilateral Partnership against Cyber Threats (IMPACT), backed by the United Nations International Telecommunication Union (ITU) and the International Criminal Police Organization (Interpol), is known as “the world’s first global public-private partnership against cyber threats”.\(^{1433}\) IMPACT is committed to promoting international cooperation in cybersecurity and building a bridge between domestic and international measures to combat cybercrime. For instance, it can operate as an anti-cyberterrorism intelligence sharing center, prompting 191 member states to strengthen international cooperation to counter cyberterrorism threats, such as defense against cyber attacks on critical infrastructure such as the global financial system, power grids, nuclear power plants, and air traffic control systems.\(^{1434}\)

Apart from the above-mentioned, there are some other multilateral international cooperation between law enforcement agencies as well as other international entities that can be applied to deal with cyber terrorism: Group of 8(G-8); European Union (EU); Asia Pacific Economic Cooperation (APEC); Organization for Economic Co-operation and Development (OECD); North Atlantic Treaty Organization (NATO).\(^{1435}\)

Although the international community has established some existing conventions or legislations, they have not introduced a universally accepted definition of cyberterrorism. Now the international community “lacks a unified international legal framework, resulting in different nations proactively developing, implementing and

\(^{1432}\) Ibid


\(^{1434}\) Ibid.

\(^{1435}\) The details of these multilateral international cooperation could be found in SS Özeren, “Cyberterrorism and International Cooperation: General Overview of the Available Mechanisms to Facilitate an Overwhelming Task” in Centre of Excellence Defence Against Terrorism (ed) Responses to Cyber Terrorism (IOS Press 2007) 77-83; NA Manap and PM Tehrani, ‘Cyber Terrorism: Issues in Its Interpretation and Enforcement’ (2012) 2(3) IJIEE 409-413; PM Tehrani, Cyberterrorism: The Legal and Enforcement Issues (World scientific press 2017) 80-133.
enforcing their own domestic laws to address cyberterrorism. It is arguable that this is a lack of international cooperation because it is new to some countries and involves many sensitive issues, ranging from economic competition, privacy and access to national security. However, as legal procedures and systems vary from country to country, it is justifiable to expand the current limited scope of application of international law on cyberterrorism and establish an effective international legal framework.

9.5 An Evaluation of the Absence of Specific Legislation on Cyberterrorism

Having explored legal responses to cyberterrorism, with a particular focus on jurisdictions of China and E&W that do not have specific anti-cyberterrorism legislation to deal with the issue, we can summarize the positive and negative aspects of the current legal framework.

As for the positive aspect, due to the lack of special anti-cyberterrorism law, it has allowed states to respond to the issue at speed; it allows states to continually adapt to the changing nature of the threat of cyberterrorism. For example, both China and E&W have criminalised a wide range of terrorism precursor offences, aggravated punishment for terrorism-related offences, empowered the executive organs with broad discretion to designate proscribed terrorist organisations and gradual extension of executive powers.

Additionally, regarding the negative aspect, due to the lack of special anti-cyberterrorism law, it relies on the existing anti-terrorism laws to combat cyberterrorism, which can lead to ill-defined and open to significant interpretation; little oversight or accountability; no transparency; etc. For example, as shown in Chapter 8, there are a

---

1439 The details could be found in Chapter 8, section 8.3.
number of problems in legal responses to cyberterrorism in China and E&W, notably over-criminalization, unpredictability, lack of counterbalance, violation of proportionality and arbitrary expansion of executive powers.  

9.6 Conclusion

The purpose of this chapter was to succinctly and clearly present some conjectures to explain the similarities and differences in the legal responses to cyberterrorism between different jurisdictions, which should be of great significance for future research on the relationship between legal systems and legal responses. Its implications for comparative social-legal studies include the need to account for developments in the social context of these systems that might better explain convergence as well as divergence in legal responses to global challenges in a more intensively, if not ‘hyper,’ connected world.

As demonstrated in previous sections, these conjectures raise some prospective research agendas explaining convergence as well as divergence in legal responses to global threats (such as cyberterrorism). The convergence of legal responses to transnational threats in different jurisdictions might derive from: pressure from supranational institutions (such as the UN and the EU); demands for the promotion of international cooperation; and the transplantation of legislation and policy between different jurisdictions. Meanwhile, the differences in the legal approaches in different jurisdictions in response to global threats stem from: resistance from ‘net importers’ of legal responses originating in other nation-states; and political power in the competition amongst rival centres of governance both within as well as between nation-states and their jurisdictions of sovereign writ.

1440 The details could be found in Chapter 8, section 8.3.
Appendix

Translation of the terrorism-related offences in the Criminal Law of the People's Republic of China《中华人民共和国刑法》

Article 2: The tasks of the PRC Criminal Law are to use punishment struggle against all criminal acts to defend national security, the political power of the people's democratic dictatorship, and the socialist system; to protect state-owned property and property collectively owned by the laboring masses; to protect citizens' privately owned property; to protect citizens' right of the person, democratic rights, and other rights; to maintain social and economic order; and to safeguard the smooth progress of the cause of socialist construction.

Article 3: Any act deemed by explicit stipulations of law as a crime is to be convicted and given punishment by law and any act that no explicit stipulations of law deems a crime is not to be convicted or given punishment.

Article 5: The severity of punishments must be commensurate with the crime committed by an offender and the criminal responsibility he bears.

Article 13: All acts that endanger the sovereignty, territorial integrity, and security of the state; split the state; subvert the political power of the people's democratic dictatorship and overthrow the socialist system; undermine social and economic order; violate property owned by the state or property collectively owned by the laboring masses; violate citizens' privately owned property; infringe upon citizens' rights of the person, democratic rights. and other rights; and other acts that endanger society, are crimes if according to law they should be criminally punished. However, if the circumstances are clearly minor and the harm is not great, they are not to be deemed crimes.

Article 22: Preparation for a crime is preparation of the instruments or creation of the conditions for the commission of a crime.

One who prepares for a crime may, in comparison with one who consummates the

crime, be given a lesser punishment or a mitigated punishment or be exempted from punishment.

Article 65: Where a convict sentenced to fixed-term imprisonment or a heavier penalty commits again a crime for which a fixed-term imprisonment or a heavier penalty shall be given within five years after finishing serving his sentence or being pardoned, he shall be a recidivist and be given a heavier penalty, unless it is a negligent crime or he commits the crime under the age of 18.

Article 66: A convict of jeopardizing the national security, terrorist activities or organized crime of a gangland nature shall be punished as a recidivist for any of such crimes committed again by him at any time after he finishes serving his sentence or is pardoned.

Article 120: Whoever organizes or leads a terrorist organization shall be sentenced to imprisonment of not less than ten years or life imprisonment and a forfeiture of property; whoever actively participates in a terrorist organization shall be sentenced to imprisonment of not less than three years but not more than ten years in addition to a fine; and other participants shall be sentenced to imprisonment of not more than three years, criminal detention, surveillance or deprivation of political rights and may be fined in addition.

Whoever commits the crime as provided for in the preceding paragraph and also commits murder, explosion, kidnapping or any other crime shall be punished according to the provisions on the joinder of penalties for plural crimes.

Article 120a: Any individual who provides financial support to a terrorist organization or conducts terrorist activities, or provides training on terrorist activities shall be sentenced to imprisonment of not more than five years, criminal detention, surveillance or deprivation of political rights in addition to a fine; or if the circumstances are serious, be sentenced to imprisonment of not less than five years in addition to a fine or forfeiture of property.

Whoever knowingly recruits, trains or transports any member workforce for any terrorist organization, for conducting any terrorist activities or for any terrorist activities shall be punished in accordance with the provisions of the preceding paragraph.
Where an entity commits a crime as provided for in the preceding two paragraphs, a fine shall be imposed on the entity, and the directly responsible person in charge and other directly liable persons shall be punished in accordance with the provisions of paragraph 1.

Article 120b: Whoever falls under any of the following circumstances shall be sentenced to imprisonment of not more than five years, criminal detention, surveillance or deprivation of political rights in addition to a fine; or be sentenced to imprisonment of not less than five years in addition to a fine or forfeiture of property if the circumstances are serious.

(1) Preparing lethal weapons, hazardous articles or other tools for conducting terrorist activities.

(2) Organizing training on terrorist activities or actively participating in training on terrorist activities.

(3) Contacting any overseas terrorist organization or person for the purpose of conducting terrorist activities.

(4) Making a plan or any other preparation for conducting terrorist activities.

Whoever commits any other crime while committing a crime as provided for in the preceding paragraph shall be convicted and punished according to the provisions on the crime with the heavier penalty.

Article 120c: Advocating terrorism or extremism through methods such as producing or distributing items such as books or audio-visual materials advocating terrorism; or advocating terrorism or extremism by giving instruction or releasing information; or inciting the perpetration of terrorist activity; is sentenced to up to five years imprisonment, short-term detention, controlled release or deprivation of political rights and a concurrent fine; where circumstances are serious, the sentence is five or more years imprisonment and a concurrent fine or confiscation of property.

Article 120d: Using extremism to incite or coerce the masses to undermine the implementation of legally established systems such as for marriage, justice, education or social management is sentenced to up to three years imprisonment, short-term
detention or controlled release and a concurrent fine; where circumstances are serious, the sentence is between three and seven years imprisonment and a concurrent fine; where circumstances are especially serious, the sentence is seven or more years imprisonment and a concurrent fine or confiscation of property.

Article 120e: Where methods such as violence or coercion are used to compel others to wear or adorn themselves with apparel or emblems promoting terrorism or extremism, it is punished by up to three years imprisonment, short-term detention or controlled release, and a concurrent fine.

Article 120f: Illegally possessing books, audio-visual materials or other materials the one clearly knows advocate terrorism or extremism, where the circumstances are serious, is punished by up to three years imprisonment, short-term detention or controlled release and/or a fine.

Article 291a: Whoever makes up any false information on the situation of any risk, epidemic disease, disaster or emergency and spreads such information on the information network or any other media, or knowingly spreads the aforesaid false information on the information network or any other media, which seriously disrupts the public order, shall be sentenced to imprisonment of not more than three years, criminal detention or surveillance; and if serious consequences have resulted, shall be sentenced to imprisonment of not less than three years but not more than seven years.

Translation of relevant provisions of Counter-Terrorism Law of the People's Republic of China 《中华人民共和国反恐怖主义法》

Article 1: For purposes of preventing and punishing terrorist activities, improving counterterrorism work, and safeguarding national security, public security and the security of people's lives and property, this Law is developed in accordance with the Constitution.

Article 3: For the purpose of this Law, “terrorism” means any proposition or activity that,
by means of violence, sabotage or threat, generates social panic, undermines public
security, infringes upon personal and property rights, or menaces state authorities and
international organizations, with the aim to realize political, ideological and other
purposes.

For the purpose of this Law, “terrorist activities” means the following conduct of the
terrorist nature:

(1) Organizing, planning, preparing for, or conducting the activities which cause or
attempt to cause casualties, grave property loss, damage to public facilities, disruption
of social order and other serious social harm.

(2) Advocating terrorism, instigating terrorist activities, or illegally holding articles
advocating terrorism, or forcing other persons to wear costume or symbols advocating
terrorism in public places.

(3) Organizing, leading or participating in terrorist organizations.

(4) Providing information, funds, materials, labor services, technologies, places and
other support, assistance and convenience to terrorist organizations, terrorists, the
implementation of terrorist activities or training on terrorist activities.

(5) Other terrorist activities.

For the purpose of this Law, “terrorist organizations” means criminal organizations
formed by three or more persons for the purpose of conducting terrorist activities.

For the purpose of this Law, “terrorists” means the individuals who conduct terrorist
activities and members of terrorist organizations.

For the purpose of this Law, “terrorist incidents” means terrorist activities that are
occurring or have occurred, which cause or may cause serious social harm.

Article 5: Counterterrorism work shall be conducted under the principles of combining
specialized tasks with reliance on the masses, giving priority to prevention, integrating
punishment and prevention, anticipating the enemy and maintaining activeness.

Article 6: Counterterrorism work shall be conducted in accordance with the law by
respecting and safeguarding human rights and protecting the lawful rights and interests of citizens and organizations.

In counterterrorism work, citizens’ freedom in religious belief and ethnic customs shall be respected, and any discriminatory deeds based on regions, ethnic groups, religions and other causes shall be prohibited.

Article 8: Public security authorities, national security authorities, people's procuratorates, people's courts, judicial administrative authorities, and other relevant state authorities shall, according to their division of work, implement the work responsibility system, and effectively conduct counterterrorism work in accordance with the law.

The Chinese People's Liberation Army, the Chinese people's armed police force and militia organizations shall prevent and punish terrorist activities in accordance with this Law and other relevant laws, administrative regulations, military regulations and orders of the State Council and the Central Military Commission, and according to the arrangements of counterterrorism leading bodies.

The relevant departments shall establish the joint cooperation mechanism, and rely on and mobilize villagers' committees, neighborhood committees, enterprises and public institutions, and social organizations to jointly conduct counterterrorism work.

Article 12: The national counterterrorism leading body shall, in accordance with the provision of Article 3 of this Law, determine terrorist organizations and individuals, and the announcement thereon shall be made by the working body of the national counterterrorism leading body.

Article 15: A determined terrorist organization or individual that has any objection to the determination may file an application for review with the working body of the national counterterrorism leading body. The national counterterrorism leading body shall conduct review in a timely manner and make a decision to maintain or revoke the determination. The review decision shall be final.

Where the national counterterrorism leading body makes a decision to revoke the determination, the working body of the national counterterrorism leading body shall
make an announcement; and the funds and assets that have been frozen shall be unfrozen.

Article 18: Telecommunications business operators and Internet service providers shall provide technical interface, decryption and other technical support and assistance for the prevention and investigation of terrorist activities conducted by public security authorities and national security authorities in accordance with the law.

Article 19: Telecommunications business operators and Internet service providers shall, in accordance with the provisions of laws and administrative regulations, put into practice network security and information content supervision rules, and technical measures for security protection, so as to avoid the dissemination of information with any terrorist or extremist content. If they discover any information with terrorist or extremist content, they shall cease the transmission immediately, preserve relevant records, delete relevant information, and report to public security authorities or the relevant departments.

Network communications, telecommunications, public security, national security and other competent departments shall, according to the division of their powers and duties, order in a timely manner the relevant entities to cease the transmission of and delete the relevant information with any terrorist or extremist content, or close the relevant websites and terminate the provision of the relevant services. Relevant entities shall immediately enforce such orders and preserve the relevant records and assist in investigation. Competent telecommunications departments shall take technical measures to block the dissemination of information with any terrorist or extremist content available on the international Internet.

Article 53: A public security authority investigating any suspected terrorist activity may, with the approval of the person in charge of the public security authority at or above the county level, order the suspect of terrorist activities to observe one or more of the following restrictive measures based on the degree of danger.

(1) The suspect shall not leave the city or county where he or she resides or the designated domicile without the approval of the public security authority.

(2) The suspect shall not participate in large-scale mass activities or engage in specific
activities.

(3) The suspect shall not take public means of transport or enter specific places without the approval of the public security authority.

(4) The suspect shall not meet or communicate by letter with specific persons.

(5) The suspect shall report the information on activities to the public security authority on a periodical basis.

(6) The suspect shall hand over the passport and other entry and exit certificates, identity certificate, and driving certificate to the public security authority for preservation.

The public security authority may take electronic monitoring, inspection from time to time and other means to oversee the suspect's compliance with restrictive measures.

The time period for taking restrictive measures prescribed in the preceding two paragraphs shall not exceed three months. If it is unnecessary to continue taking restrictive measures, the measures shall be removed in a timely manner.

Article 76: Where the personal safety of a person or any of his or her close relatives is endangered for the reason of reporting or stopping any terrorist activity, testifying in a criminal case on terrorist activities or conducting counterterrorism work, upon the application of the person or his or her close relative, the public security authority and the relevant departments shall adopt one or more of the following protective measures:

(1) Not disclosing the personal information such as the true name, address and employer

(2) Prohibiting any specified person from approaching the protected person.

(3) Taking special protective measures for a person or residence.

(4) Modifying the name of the protected person and arranging a new domicile and workplace.

(5) Other necessary protective measures.

The public security authority and the relevant departments shall, according to the
provisions of the preceding paragraph, not disclose the true name or address of the protected entity, prohibit specific persons from approaching the protected entity, take special protective measures for the office and business premises of the protected entity, and take other necessary protective measures.

Article 80: Where anyone participates in any of the following activities, and the circumstances are not serious enough to constitute a crime, he or she shall be detained by the public security authority for not less than ten days but not more than 15 days, and may be concurrently fined not more than 10,000 yuan.

(1) Advocating terrorism or extremism, or instigating any terrorist or extremist activity.
(2) Producing, spreading or illegally holding any articles advocating terrorism or extremism.
(3) Forcing any other person to wear costume or symbols advocating terrorism or extremism in a public place.
(4) Providing information, funds, materials, labor services, technologies, places and other support, assistance and convenience for advocating terrorism or extremism or the implementation of any terrorist or extremist activity.

Article 81: Where anyone commits any of the following conduct by using extremism, and the circumstances are not serious enough to constitute a crime, he or she shall be detained by the public security authority for not less than five days but not more than 15 days, and may be concurrently fined not more than 10,000 yuan.

(1) Forcing any other person to join any religious activity, or forcing any other person to make donations or provide labor services to any place of religious worship or to clergies.
(2) Ousting persons of other ethnic groups or faiths from their domiciles by threat, harassment or other means.
(3) Interfering with others' relationships or living with persons of different ethnic groups or faiths by threat, harassment or other means.
(4) Interfering in the habits and ways of life of other persons, or in production or
business operation by threat, harassment or other means.

(5) Obstructing the lawful performance of functions by any staff member of a state authority.

(6) Distorting or defaming any state policy, law, administrative regulation, or inciting or instigating others to resist lawful administration by the people's government.

(7) Instigating or forcing people to damage, or intentionally damage residents’ identification cards, household certificates and other legal documents of the state, and RMB.

(8) Instigating or forcing any other person to replace marriage or divorce registration with any religious rites.

(9) Instigating or forcing any minors not to receive compulsory education.

(10) Otherwise disrupting the implementation of the legal system of the state by using extremism.

Article 82: Where anyone harbors or shields any person although knowing that the latter commits any terrorist or extremist offense, and the circumstances are not serious enough to constitute a crime, or if anyone refuses to provide the relevant evidence when the judicial authority investigates the relevant information and collects the relevant evidence from him or her, the public security authority shall detain the violator for not less than ten days but not more than 15 days, and may impose a fine of not more than 10,000 yuan on the violator.

Article 84: Where a telecommunications business operator or an Internet service provider falls under any of the following circumstances, the competent department shall impose a fine of not less than 200,000 yuan but not more than 500,000 yuan on the violator, and impose a fine of not more than 100,000 yuan on its directly responsible persons in charge and other directly liable persons; and if the circumstances are serious, impose a fine of not less than 500,000 yuan on the violator, and impose a fine of not less than 100,000 yuan but not more than 500,000 yuan on its directly responsible persons in charge and other directly liable persons, and the public security authority may detain its directly responsible persons in charge and other directly liable
persons for not less than five days but not more than 15 days.

(1) It fails to provide technical interface, decryption and other technical support and assistance for the prevention and investigation of terrorist activities conducted by any public security authority or national security authority as required.

(2) It fails to cease the transmission and deletion of information with any terrorist or extremist content, preserve the relevant records, shut the relevant website or terminate the provision of the relevant services according to the requirements of the competent department.

(3) It fails to implement network security, information content supervision rules or technical measures for security prevention, which causes the dissemination of information with any terrorist or extremist content, and the circumstances are serious.

Article 85: Where any entity providing cargo transport by railway, highway, waterway or air, postal entity, express delivery entity, or any other logistics operation entity falls under any of the following circumstances, the competent department shall impose a fine of not less than 100,000 yuan but not more than 500,000 yuan on the entity, and impose a fine of not more than 100,000 yuan on its directly responsible persons in charge and other directly liable persons.

(1) It fails to implement security check rules, or check clients' identities, or fails to conduct security check or visual check of the articles transported and delivered as required.

(2) It transports or delivers any articles prohibited from transport and delivery, articles with serious potential safety hazards, or articles on which clients refuse to accept security check.

(3) It fails to implement rules on the registration of information on identities of clients who transport and deliver articles and information on articles.

Article 86: Where a business operator or service provider in telecommunications, Internet or finance fails to check clients' identities as required, or provides services to any client whose identity is not clear or who refuses to accept identity check, the competent authority shall order the violator to make correction; if the violator refuses
Article 87: Where anyone falls under any of the following circumstances in violation of the provisions of the Law, the competent department shall give the violator a warning and order it to make correction; and if it refuses to make correction, impose a fine of not more than 100,000 yuan on the violator, and impose a fine of not more than 10,000 yuan on its directly responsible persons in charge and other directly liable persons.

(1) It fails to produce electronic track labels on guns or any other weapon, ammunition, controlled instruments, hazardous chemicals, or nuclear and radioactive articles as required.

(2) It fails to monitor the transport vehicles of hazardous chemicals, civil explosives, or nuclear and radioactive articles in operation through the positioning system as required.

(3) It fails to conduct strict supervision and administration of infectious pathogens or any other substance as required, and the circumstances are serious.

(4) It violates the measure of controlling or restricting the trading of controlled instruments, hazardous chemicals or civil explosives as decided by the relevant department of the State Council or the provincial people's government when the circumstances are serious.

Article 88: Where an entity managing or operating a key target for potential terrorist attack falls under any of the following circumstances in violation of the provisions of the Law, the competent department shall give the violator a warning and order it to make correction; and if it refuses to make correction, impose a fine of not more than 100,000 yuan on the violator, and impose a fine of not more than 50,000 yuan on its directly responsible persons in charge and other directly liable persons.

Where a business operator or service provider in accommodation, long-distance passenger transport, or motor vehicle lease, among others, falls under any of the circumstances prescribed in the preceding paragraph, the competent department shall impose a fine of not less than 100,000 yuan but not more than 500,000 yuan on the violator, and impose a fine of not less than 100,000 yuan but not more than 500,000 yuan on its directly responsible persons in charge and other directly liable persons.
this Law, the public security authority shall give the entity a warning and order it to make correction; and if it refuses to make correction, impose a fine of not more than 100,000 yuan on the entity, and impose a fine of not more than 10,000 yuan on its directly responsible persons in charge and other directly liable persons.

(1) It fails to make advance plans and formulate measures for preventing, responding to and handling terrorist activities.

(2) It fails to establish rules for guaranteeing special counterterrorism work fund, or equip itself with the equipment and facilities for prevention and handling.

(3) It fails to assign the working body or responsible personnel.

(4) It fails to conduct security background review of personnel on key posts, or fails to transfer the personnel who are inappropriate to other posts.

(5) It fails to provide security personnel and related equipment and facilities to public means of transport as required.

(6) It fails to establish management rules for the monitoring, information preservation and use, operation and maintenance of the public security video information system.

Where any entity undertaking large-scale activities or any entity managing a key target fails to conduct security check of people, articles and means of transport entering any place for holding large-scale activities, airport, train station, dock, urban rail transit station, long-distance bus station, port or any other key target, the public security authority shall order the entity to make correction; and if it refuses to make correction, impose a fine of not more than 100,000 yuan on the entity, and impose a fine of not more than 10,000 yuan on its directly responsible persons in charge and other directly liable persons.

Article 89: Where any suspect of terrorist activities fails to comply with the restrictive measures which the public security authority orders him or her to comply with, the public security authority shall give the suspect a warning and order the suspect to make correction; and if the suspect refuses to make correction, it shall detain the suspect for not less than five days but not more than 15 days.
Article 90: Where news media or any other entity fabricates or spreads any false information on terrorist incidents, reports or spreads any details of terrorist activities that may trigger imitation, issues any cruel or inhuman scene in a terrorist incident, or reports or spreads, without approval, the identity information on on-site response and handling personnel and hostage and the response and handling information, the public security authority shall impose a fine of not more than 200,000 yuan on it, and detain its directly responsible persons in charge and other directly liable persons for not less than five days but not more than 15 days, and may concurrently impose a fine of not more than 50,000 yuan on them.

Where any individual commits any conduct as prescribed in the preceding paragraph, the public security authority shall detain the individual for not less than five days but not more than 15 days, and may concurrently impose a fine of not more than 10,000 yuan on the individual.

Article 91: Where anyone refuses to cooperate in counterterrorism security protection, intelligence information, investigation, and response and handling conducted by the relevant department, the competent department shall impose a fine of not more than 2,000 yuan on the violator; and if any serious consequence is caused, detain the violator for not less than five days but not more than 15 days, and may concurrently impose a fine of not more than 10,000 yuan on the violator.

Where an entity commits any conduct as prescribed in the preceding paragraph, the competent department shall impose a fine of not more than 50,000 yuan on the entity; and if any serious consequence is caused, impose a fine of not more than 100,000 yuan on the entity; and punish its directly responsible persons in charge and other directly liable persons in accordance with the provisions of the preceding paragraph.

Article 92: Where anyone obstructs the relevant department's counterterrorism work, the public security authority shall detain the violator for not less than five days but not more than 15 days and may concurrently impose a fine of not more than 50,000 yuan on the person.

Where an entity commits any conduct as prescribed in the preceding paragraph, the public security authority shall impose a fine of not more than 200,000 yuan on the entity.
and punish its directly responsible persons in charge and other directly liable persons in accordance with the provisions of the preceding paragraph.

Whoever obstructs the lawful performance of functions by the people’s police, the Chinese People’s Liberation Army, or the people’s armed police force shall be given a heavier penalty.

Article 93: Where any entity violates the provisions of this Law and the circumstances are serious, the competent department shall order the entity to cease the relevant business operation or the provision of relevant services, or order it to cease production and business operation; and if any serious consequence is caused, revoke the relevant certificate or license or revoke registration.

Translation of relevant provisions of the Criminal Procedure Law of the People’s Republic of China

Article 33: A criminal suspect shall have the right to entrust persons as defenders from the date on which the investigatory organ conduct interrogation or take mandatory measures against him for the first time. During the period of investigation, only lawyers may be entrusted as defenders. Defendants shall be entitled to entrust defenders at any moment.

The investigatory organ shall inform the criminal suspect of his right to entrust defenders when it conducts interrogation or takes mandatory measures against him for the first time. The people’s procuratorate shall do so within 3 days as of the day it receives the file record of a case transferred for examination before prosecution. The people’s court shall inform the defendant of his right to entrust a defender within 3 days from the day it entertains the case. Where a criminal suspect or a defendant under detention requires entrusting defenders, the people’s court, the people’s procuratorate and the public security organ shall forward his request promptly.

Where a criminal suspect or a defendant is in custody, his guardians or close relatives

may entrust defenders for him.

Defenders who accept entrust of the criminal suspect or the defendant shall notify promptly the relevant organs dealing with the case.

Article 73: Residential surveillance shall be executed in the domicile of the criminal suspect or defendant; if he has no such a domicile, it can be executed in a designated residence. If the criminal suspect or defendant has committed a crime endangering the state security, involving terrors or particularly major bribery, and execution in his domicile may obstruct the investigation, it may also be executed in a designated residence. However, it shall not be executed in a detention place or a special place for case handling.

Where a residence is designated for residential surveillance, the family members of the executed shall be notified within 24 hours after the execution of the residential surveillance except that it is impossible to do so.

Where the criminal suspect or defendant under residential surveillance entrusts a defender, the provision of Article 33 of this Law shall apply.

The people’s procuratorate shall surprise over the validity of the decision and execution of the residential surveillance in a designated residence.

Article 76: The executing organ may conduct an electronic monitoring or irregular inspections to monitor the criminal suspect or defendant in terms of his observation of the provisions of residential surveillance. During the investigation, the correspondence of the criminal suspect who is under residential surveillance may be monitored.

Article 83: When detaining a person, the public security organ must produce a detention a detention warrant.

Within 24 hours after a person has been detained, the detainee shall be immediately sent to house of defendant. Except in circumstances where there is no way of notifying his family or such notification would hinder the investigation because he is involved in crimes endangering the state security or terror crimes, his family shall be notified within 24 hours after he is detained. When the circumstances that hinder investigation disappear, his family shall be notified immediately.
Article 148: After setting up a case of crime endangering the state security, involving terrors, committed by mafia, related to drug or other major crimes that severely endanger the society, the public security organ may, according to the need to investigate crimes, adopt technology investigation measures through strict formalities of approval.

After setting up a case of a major crime involving embezzlement or bribery, or taking advantage of one's functions and powers to seriously infringe upon the personal rights of citizens, or other major crimes, the people's procuratorate may, according to the need to investigate crimes, adopt technical investigation measures through strict formalities of approval and deliver the case pursuant to stipulations to the relevant organs for execution.

In pursuing a criminal suspect or defendant who is wanted, or who is a fugitive and is approved or decided to be arrested, technical investigation measures that are necessary for the pursuit may be adopted upon approval.

Article 150: The technical investigation measures must be implemented strictly according to the category, object of application and time limit approved.

The investigators shall keep secret the state secrets, trade secrets and individual privacy learned in the process of taking technical investigation measures; if the information and materials of facts obtained by technical investigation measures are irrelevant to the case, they shall be destroyed without delay.

The materials obtained by technical investigation measures shall be sued only in the investigation, prosecution and trial of the crime, and shall not be used for other purposes.

When the public security organ adopts technical investigation measures according to law, the related units and individuals shall cooperate and shall keep secret the relevant situations.

Article 153: If a criminal suspect who should be arrested is a fugitive, the public security organ may issue a wanted order and take effective measures to pursue him for arrest and bring him to justice. The public security organ at any level may directly issue
wanted orders within the area under its jurisdiction. It shall request a higher-level organ with the proper authority to issue such orders for areas beyond its jurisdiction.

Article 154: The time limit for holding criminal suspect in custody during investigation after arrest shall not exceed two months. If the case is complex and cannot be concluded within the time limit, an extension of one month may be allowed with the approval of the people’s procuratorate at the next higher level.

Article 155: If due to special reasons, it is not appropriate to hand over a particularly grave and complex case for trial even within a relatively long period of time, the Supreme People’s Procuratorate shall submit a report to the Standing Committee of the National People’s Congress for approval of postponing the hearing of the case.

Article 156: With respect to the following cases, if investigation cannot be concluded within the time limit specified in Article 153 of this Law, an extension of two months may be allowed upon approval or decision by the people’s procuratorate of a province, autonomous region or municipality directly under the Central Government.

(1) grave and complex cases in outlying areas where traffic is most inconvenient;

(2) grave cases that involve criminal gangs;

(3) grave cases and complex cases that involve people who commit crimes from one place to another;

(4) grave and complex cases that involve various quarters and for which it is difficult to obtain evidence.

Article 157: If in the case of a criminal suspect who may be sentenced to fixed-term imprisonment of ten years at least, investigation of the case can still not be concluded upon expiration of the extended time limit as provided in Article 156 of this Law, another extension of two months may be allowed upon approval or decision by the people’s procuratorate of a province, autonomous region or municipality directly under the Central Government.

People’s Police Law of the People’s Republic of China《中华人民共和国警察法》
Article 16: As necessitated by investigation of a crime, public security organs may, in accordance with relevant regulations of the State, take technical reconnaissance measures after strictly following approval formalities.

**Constitution of the People's Republic of China**

Article 2: All power in the People's Republic of China belongs to the people.

The National People's Congress and the local people’s congresses at various levels are the organs through which the people exercise state power.

The people administer state affairs and manage economic, cultural and social affairs through various channels and in various ways in accordance with the law.

Article 5: The People's Republic of China practices ruling the country in accordance with the law and building a socialist country of law.

The state upholds the uniformity and dignity of the socialist legal system.

No laws or administrative or local rules and regulations may contravene the Constitution.

All state organs, the armed forces, all political parties and public organizations and all enterprises and institutions must abide by the Constitution and the law. All acts in violation of the Constitution or the law must be investigated.

No organization or individual is privileged to be beyond the Constitution or the law.

Article 33: All persons holding the nationality of the People's Republic of China are citizens of the People's Republic of China. All citizens of the People's Republic of China are equal before the law. Every citizen is entitled to the rights and at the same time must perform the duties prescribed by the Constitution and the law.

Article 34: All citizens of the People's Republic of China who have reached the age of 18 have the right to vote and stand for election, regardless of ethnic status, race, sex, occupation, family background, religious belief, education, property status or length of residence, except persons deprived of political rights according to law.

Article 35: Citizens of the People's Republic of China enjoy freedom of speech, of the press, of assembly, of association, of procession and of demonstration.

Article 36: Citizens of the People's Republic of China enjoy freedom of religious belief. No state organ, public organization or individual may compel citizens to believe in, or not to believe in, any religion; nor may they discriminate against citizens who believe in, or do not believe in, any religion. The state protects normal religious activities. No one may make use of religion to engage in activities that disrupt public order, impair the health of citizens or interfere with the educational system of the state. Religious

---


bodies and religious affairs are not subject to any foreign domination.

Article 37: Freedom of the person of citizens of the People's Republic of China is inviolable. No citizen may be arrested except with the approval or by decision of a people's procuratorate or by decision of a people's court, and arrests must be made by a public security organ. Unlawful detention or deprivation or restriction of citizens freedom of the person by other means is prohibited, and unlawful search of the person of citizens is prohibited.

Article 38: The personal dignity of citizens of the People's Republic of China is inviolable. Insult, libel, false accusation or false incrimination directed against citizens by any means is prohibited.

Article 39: The residences of citizens of the People's Republic of China are inviolable. Unlawful search of, or intrusion into, a citizen's residence is prohibited.

Article 40: Freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law. No organization or individual may, on any ground, infringe upon citizens freedom and privacy of correspondence, except in cases where, to meet the needs of state security or of criminal investigation, public security or procuratorial organs are permitted to censor correspondence in accordance with procedures prescribed by law.

Article 41: Citizens of the People's Republic of China have the right to criticize and make suggestions regarding any state organ or functionary. Citizens have the right to make to relevant state organs complaints or charges against, or exposures of, any state organ or functionary for violation of the law or dereliction of duty; but fabrication or distortion of facts for purposes of libel or false incrimination is prohibited. The state organ concerned must deal with complaints, charges or exposures made by citizens in a responsible manner after ascertaining the facts. No one may suppress such complaints, charges and exposures or retaliate against the citizens making them. Citizens who have suffered losses as a result of infringement of their civic rights by any state organ or functionary have the right to compensation in accordance with the law.

Article 42: Citizens of the People's Republic of China have the right as well as the duty to work. Through various channels, the state creates conditions for employment, enhances occupational safety and health, improves working conditions and, on the basis of expanded production, increases remuneration for work and welfare benefits. Work is a matter of honour for every citizen who is able to work. All working people in state enterprises and in urban and rural economic collectives should approach their work as the masters of the country that they are. The state promotes socialist labour emulation, and commends and rewards model and advanced workers. The state encourages citizens to take part in voluntary labour. The state provides necessary vocational training for citizens before they are employed.

Article 43: Working people in the People's Republic of China have the right to rest. The state expands facilities for the rest and recuperation of the working people and prescribes working hours and vacations for workers and staff.

Article 44: The state applies the system of retirement for workers and staff of enterprises and institutions and for functionaries of organs of state according to law. The livelihood of retired personnel is ensured by the state and society.

Article 45: Citizens of the People's Republic of China have the right to material assistance from the state and society when they are old, ill or disabled. The state
develops social insurance, social relief and medical and health services that are required for citizens to enjoy this right. The state and society ensure the livelihood of disabled members of the armed forces, provide pensions to the families of martyrs and give preferential treatment to the families of military personnel. The state and society help make arrangements for the work, livelihood and education of the blind, deaf-mutes and other handicapped citizens.

Article 46: Citizens of the People's Republic of China have the duty as well as the right to receive education. The state promotes the all-round development of children and young people, morally, intellectually and physically.

Article 47: Citizens of the People's Republic of China have the freedom to engage in scientific research, literary and artistic creation and other cultural pursuits. The state encourages and assists creative endeavors conducive to the interests of the people that are made by citizens engaged in education, science, technology, literature, art and other cultural work.

Article 48: Women in the People's Republic of China enjoy equal rights with men in all spheres of life, in political, economic, cultural, social and family life. The state protects the rights and interests of women, applies the principle of equal pay for equal work to men and women alike and trains and selects cadres from among women.

Article 49: Marriage, the family and mother and child are protected by the state. Both husband and wife have the duty to practise family planning. Parents have the duty to rear and educate their children who are minors, and children who have come of age have the duty to support and assist their parents. Violation of the freedom of marriage is prohibited. Maltreatment of old people, women and children is prohibited.

Article 50: The People's Republic of China protects the legitimate rights and interests of Chinese nationals residing abroad and protects the lawful rights and interests of returned overseas Chinese and of the family members of Chinese nationals residing abroad.

Article 51: Citizens of the People's Republic of China, in exercising their freedoms and rights, may not infringe upon the interests of the state, of society or of the collective, or upon the lawful freedoms and rights of other citizens.

Article 52: It is the duty of citizens of the People's Republic of China to safeguard the unification of the country and the unity of all its nationalities.

Article 53: Citizens of the People's Republic of China must abide by the Constitution and the law, keep state secrets, protect public property, observe labour discipline and public order and respect social ethics.

Article 54: It is the duty of citizens of the People's Republic of China to safeguard the security, honour and interests of the motherland; they must not commit acts detrimental to the security, honour and interests of the motherland.

Article 55: It is the sacred duty of every citizen of the People's Republic of China to defend the motherland and resist aggression. It is the honorable duty of citizens of the People's Republic of China to perform military service and join the militia in accordance with the law.

Article 56: It is duty of citizens of the People's Republic of China to pay taxes in accordance with the law.

Article 57: The National People's Congress of the People's Republic of China is the
highest organ of state power. Its permanent body is the Standing Committee of the National People’s Congress.

Article 126: The people’s courts exercise judicial power independently, in accordance with the provisions of the law, and are not subject to interference by any administrative organ, public organization or individual.

Article 127: The Supreme People’s Court is the highest judicial organ. The Supreme People’s Court supervises the administration of justice by the people's courts at various local levels and by the special people’s courts. People's courts at higher levels supervise the administration of justice by those at lower levels.

Article 128: The Supreme People’s Court is responsible to the National People's Congress and its Standing Committee. Local people's courts at various levels are responsible to the organs of state power which created them.

Article 129: The people’s procuratorates of the People's Republic of China are state organs for legal supervision.

Legislation Law of the People's Republic of China 《中华人民共和国立法法》

Article 90: When the State Council, the Central Military Commission, the Supreme People’s Court, the Supreme People’s Procuratorate and the standing committees of the people's congresses of the provinces, autonomous regions and municipalities directly under the Central Government consider that administrative regulations, local regulations, autonomous regulations or separate regulations contradict the Constitution or laws, they may submit to the Standing Committee of the National People's Congress written requests for examination, and the working offices of the Standing Committee shall refer the requests to the relevant special committees for examination and suggestions.

When State organs other than those mentioned in the preceding paragraph, public organizations, enterprises and institutions or citizens consider that administrative regulations, local regulations, autonomous regulations or separate regulations contradict the Constitution or laws, they may submit to the Standing Committee of the National People's Congress written suggestions for examination, and the working offices of the Standing Committee shall study the suggestions and shall, when necessary, refer them to the relevant special committees for examination and suggestions.

National Security Law of the People’s Republic of China 《中华人民共和国国家安全法》

Article 10: The preservation of national security shall persist in mutual trust, mutual

---


benefit, equality and coordination; actively developing security exchanges and cooperation with foreign governments and international organizations, performing international security obligations, promoting common security and maintaining world peace.

Rules of Criminal Procedure of the People's Procuratorate of the People's Republic of China

Article 52: Where after the case is transferred for review for indictment, defense counsel applies for the collection or gathering evidence pursuant to the first clause of Article 41 of the Criminal Procedure Law, the case management department of People's Procuratorate shall promptly transfer the application materials to the prosecution department.

Where the people's procuratorate considers it necessary to collect or gather evidence, it shall decide to do so and make notes to attach to case file; if deciding not to collect or gather evidence it shall provide a written explanations of the reasons.

The defense counsel may be present when the people's procuratorate collects and obtains evidence in accordance with defense counsel's request.

---

Bibliography

A v Secretary of State for the Home Department [2004] UKHL 56

Ackerman B, ‘Before the Next Attack - Preserving Civil Liberties in an Age of Terrorism’ (2007) PL 181


Alder J, Constitutional and Administrative Law (7th edn, Palgrave Macmillan 2009)


--‘A Second Great Wall?: China’s Post-Cultural Revolution Project of Legal Construction’ (1999) 11(2) CD198


Allan TRS, Constitutional Justice: A Liberal Theory of the Rule of Law (OUP 2003) 31


Anderson PH, 'A Minnesota Judge's Perspective on the Rule of Law in China and Kyrgyzstan' (2009) 18 MJIL 343


-- ‘Four Threats to the Presumption of Innocence’(2006) 10(4) IJEP 241

-- ‘Conceptions of Overcriminalization’(2008) 5 OSJCL 407


-- ‘The Unfairness of Risk-based Possession Offences’. (2011) 5(3) CLP 237

-- Positive Obligations in Criminal Law (Bloomsbury Publishing 2013)

-- and Horder J, Principles of Criminal Law (7th edn, Oxford University Press 2013)

Ashworth A and Zedner L, ‘Just Prevention: Preventive Rationales and the Limits of the Criminal Law’ in RA Duff and SP Green(eds), Philosophical Foundations of the Criminal (OUP 2011)

-- ‘Prevention and Criminalization: Justifications and Limits’ (2012) 15 NCLR 542

-- and Tomlin P (eds), Prevention and the Limits of the Criminal Law (Oxford University Press 2013)

-- ‘Punishment Paradigms and the Role of the Preventive Stage’ in AP Simester, U Neumann and AD Bois-Pedain(eds), Liberal Criminal Theory: Essays for Andreas von...
Hirsch (Hart Publishing 2014)

-- Preventive Justice (Oxford University Press 2014)


Ayres I and Braithwaite J, Responsive Regulation: Transcending the Deregulation Debate (Oxford University Press)

Bagehot W, The English Constitution (Oxford 2001)


-- ‘Having One's Cake and eating it: The Paradox of Contextualization in Socio-legal Research’ (2011) 7(4) IJLC 487

Banaker R and Travers M (eds), Theory and Method in Socio-Legal Research (Hart Publishing 2005)


Barendt E, 'Incitement to, and Glorification of, Terrorism’ in I Hare and J Weinstein (ed), Extreme Speech and Democracy (Oxford University Press 2009)

-- Freedom of Speech (OUP 2005)

Barnett H, Constitutional and Administrative Law (9th edn, Routledge 2011)


Bayley DH and Weisburd D, ‘Cops and spooks: The role of the police in counterterrorism’, in D Weisburd and others (eds), To Protect and to Serve: Police and Policing in an Age of Terrorism – and Beyond (Springer 2009)


Beccaria C, On Crimes and Punishments, translated by Henry Paolucci (Bodds-Merrili 1963)


Becquelin N, ‘Criminalizing Ethnicity: Political Repression in Xinjiang’ (2004) 39(1) CRF1


Beetham D, Defining and Measuring Democracy (Sage 1994)

Beghal (Appellant) v Director of Public Prosecutions (Respondent) [2015] UKSC 49

Behr IV and others, Radicalization in the Digital Era (Rand 2013)


Bellamy R (ed), Beccaria On Crimes and Punishments and Other Writings (Cambridge University Press 1995)


Bianchi A, Enforcing International Norms against Terrorism (Hart 2004)

-- ‘Assessing the effectiveness of the UN security council’s Anti-terrorism measures:the quest for legitimacy and cohesion’ (2006)17 EJIL 881


-- The Rule of Law (Penguin 2011)

-- ‘The Rule of Law’ in D Bates (ed), The Rule of Law: The Sixth Sir David Williams
Lecture(Cambridge Law 2018)


Blum S, ‘Preventive Detention in the War on Terror. A Comparison of How the United States, Britain and Israel Detain and Incapacitate Terrorist Suspects’ (2008) 4(3) HSA 1


Bradley AW and Ewing KD, Constitutional and Administrative Law (15th edn, Pearson 2011)

Brewster D, ‘Crime Control in Japan: Exceptional, Convergent or What Else?’ (2020) 60 (6) BJC 1547


Brunst PW, ‘Use of the Internet by Terrorist—A Threat Analysis’ in Center of Excellence Defence against Terrorism(ed), Research to Cyber Terrorism (IOS Press 2008)


Burton J, ‘A Section Too Far?’ (2008) 37(3)IC 115


Cabinet Office, The national security strategy: a strong Britain in an age of uncertainty(Cm 7953,2010)


-- The Definition of Terrorism (Cmd 7052, 2007)


Castillo Petruzzi and others v Peru [1999] IACHR 6 (30 May 1999)
Centre of Excellence Defence Against Terrorism, *Responses to Cyber Terrorism* (IOS press, 2007)

Chaliand G and Blin A, *The History of Terrorism from Antiquity to Al Qaeda* (University of California Press 2007)


Chase OG, ‘Legal Processes and National Culture’ (1997) 5 CJICL 1


Chen TM, Jarvis L and Macdonald S(eds), *Cyberterrorism: Understanding, Assessment and Response* (Springer 2014)


-- *Normative Criminal Law* (规范刑法学) (Renmin University Press 2013)


Cheng Xin, ‘Research on Cyber Terrorism Crimes and Preventive Countermeasures(网络恐怖主义犯罪行为及防范对策研究)’ (Master thesis, Northwest University 2010)


China Daily, ‘the report of the SPC and SPP targeted to violent terrorism offences, no one is immune from terrorism(两高报告剑指暴恐犯罪 面对恐怖主义谁都不能独善其身 )’(China Daily, 13 March 2015)<http://www.chinadaily.com.cn/dfpd/xj/2015-03/13/content_19802124.htm>accessed 20 Sep 2020

China Institute of Contemporary International Relations, *Yearbook of International Terrorism and Counter-terrorism annually* (国际恐怖主义与反恐怖斗争) (Current Affairs Press 2017)
China Judgements Online, ‘Criminal Judgment of the Intermediate People’s Court of Dalian, Liaoning’ (<http://wenshu.court.gov.cn/list/list/?sorttype=1&number=CRNVFE8U&guid=dc1e0a4c-2dd4-d04bfa4a-eecc3064f38e&conditions=searchWord+QWJS+++全文检索;煽动民族仇恨> accessed 20 July 2020

China Judgements Online, <http://wenshu.court.gov.cn/website/wenshu/181217BMTKHNT2W0/index.html?pageId=93814f0e018f425935c85a6e4a6022c3&s21=%E6%81%90%E6%80%96%E4%B8%BB%E4%B9%89> accessed 1 Oct 2019


China’s Supreme People’s Court, ‘Verdict of Aini Aisan for Murder, Organisation and Planning Terrorist Attacks(艾尼·艾叁等故意杀人、组织、领导恐怖组织死刑复核刑事裁定书）’(<Court.gov.cn, 10 Sep 2015) <http://www.court.gov.cn/paper/content/view/id/9587.html> accessed 8 November 2020


-- and Fenwick H, ‘The impact of counter-terrorism measures on Muslim communities’ (2011) 25(3) IRLCT 151

Chow DCK and Han AM, Doing Business in China: Problems, Cases, And Materials (West Academic Publishing 2012)


Clarke M, ‘Widening the net: China’s anti-terror laws and human rights in the Xinjiang Uyghur Autonomous’ (2010) 14(4) IJHR 542

-- Terrorism and Counter-terrorism in China: Domestic and Foreign Policy Dimensions (Oxford University 2018)


Colarik A, Cyber Terrorism Political and Economic Implications (Idea Group Publishing, 2006)


Concluding Observations of the UN Human Rights Committee, ‘Egypt’ (9 August 1993) Doc CCPR/C/79/Add.23


-- ‘Algeria’ (18 August 1998) UN Doc CCPR/C/79/Add.95


-- ‘Democratic Peoples’ Republic of Korea’ (27 August 2001) UN Doc CCPR/CO/72/PRK

-- ‘United States of America’ (15 September 2006) UN Doc CCPR/C/USA/CO/3


Congreve v Secretary of State for the Home Office [1976] QB 629, [1976] 1 All ER 697


-- ‘Hackers as Terrorists? Why it doesn’t Compute’ (2003) 12CFS 10

-- ‘Cyberterrorism: Media Myth or Clear and Present Danger?’ in J Irwin (ed), War and Virtual War: the Challenges to Communities (Rodopi 2004)

-- ‘Reality Check: Assessing the (un)likelihood of Cyberterrorism’ in T Chen, L Jarvis, S Macdonald (eds), Cyberterrorism: Understanding, Assessment, and Response (Springer 2014)

Costa RS, ‘Brazil’ in K Roach (ed), Comparative Counter-Terrorism Law (Cambridge University 2015)

-- ‘The Concept of Legal Culture’ in D Nelken(ed), *Comparing Legal Cultures: Socio-legal studies series* (Dartmouth1997)


Counter-Terrorism and Security Bill, HC Second Reading (2014) Col 263


Cox R, ‘Social Forces, States and World Orders: Beyond International Relations Theory’ (1981) 10 (2)MJIS126, 126–155;


D’Amato A, ‘Legal Uncertainty’ (1983) 71 CLR 1

Da Costa [2009] EWCA Crim 482


Dannemann G, ‘Comparative Law: Study of Similarities or Differences?’ in M Reimann and R Zimmerman (eds), The Oxford Handbook of Comparative Law (OUP 2006)


Davis EVW, ‘Uyghur Muslim Ethnic Separatism in Xinjiang’ (2008) 35(1)AAAR15


deFreitas v Secretary of Ministry of Agriculture, Fisheries, Lands and Housing [1999] 1 AC 69


-- ‘On the problem of reform of political system(关于政治体制改革问题)’ and ‘Emancipate the mind, seek the truth from facts and unite as one in looking to the future(解放思想,事实就是,团结一致向前看)’ in Deng Xiaoping, Selected Works of Deng Xiaoping (People Publishing 1993)

-- Selected Work of Deng Xiaoping (邓小平文选) (Renmin Press 1994)

Denning DE, ‘Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy’ in J Arquilla and D Ronfeldt’s (eds), Networks and Netwars: The Future of Terror, Crime, and Militancy (RAND Corporation 2001)

-- ‘Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services US House Representatives’ (Georgetown University, 10 October 2003) < http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html> accessed 21 May 2020)

-- ‘Cyberterrorism Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives’ in EV Linden(ed), Focus on Terrorism (Nova Publishers 2007)

Dershowitz A, The Case for Pre-Emption (W.W. Norton 2006)

-- Preemption: A knife that cuts both ways (W.W. Norton & Company 2007)
Derwalt LMV, *Comparative Method: Comparing Legal Systems or Legal Culture* (Speculum Juris 2006)


--- *An Introduction to the Study of the Law of the Constitution* (9th edn, Macmillan 1945)


Dobinson I and Johns F, ‘Qualitative Legal Research’ in M McConville and Wing Hong Chui (eds), *Research Methods for Law* (Edinburgh University Press 2007)

Dogrul M, Aslan A, Celik E, ‘Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism’ (3rd International Conference on Cyber Conflict, Estonia, 2011)


Douglas R, ‘Must terrorists act for a cause? The motivational requirement in definitions of terrorism in the United Kingdom, Canada, New Zealand and Australia’ (2010) 36(2) CLB 295


Dowell WT, ‘The internet, censorship, and China’ (2016) 7 GJIIA 111

DPP v Collins [2007] 1 Cr App R 5


--- ‘Coordination in Counter-Terrorism (反恐领域的行刑衔接)’ (2016) 24 (5) Journal of National Prosecutors College 22
-- ‘Study of ‘Double Track’ System of Terrorist Organisations and Individuals in China
中国恐怖活动组织和人员认定‘双轨制’研究’ (2016) 32 (1) Journal of Chinese People’s
Public Security University(Social Sciences Edition) 67

Du Xiaofei, ‘Research on Anti-terrorism Legislation in the UK(英国反恐立法研究)’( Master thesis, Shandong University 2011)

Duff RA, Answering for Crime: Responsibility and Liability in the Criminal Law(Hart
Publishing 2007)

-- Farmer L, Marshall SE, Renzo M, Tadros V (eds), The Boundaries of the Criminal
Law (Oxford University Press 2010)

-- ‘Perversions and Subversions of Criminal Law’ in RA Duff and others(eds), The
Boundaries of Criminal Law (Oxford University Press 2011)

-- ‘Presuming Innocence’ in L Zedner and Julian V Roberts(eds), Principles and values
in Criminal Law and Criminal Justice: Essays in Honour of Andrew Ashworth (OUP
2012)

-- ‘Towards a Modest Legal Moralism’ (2014) 8 CLP 217

Dui Hua, ‘China’s New Criminal Procedure Law: ‘Disappearance Clause” Revised’
criminal-procedure-law.html. >accessed 20 Sep 2020

Duncan C,’Out of Conformity: China’s Capacity to implement World Trade
Organization Dispute Settlement Body Decisions after Accession’ (2002) 18 AUILR
399

Eberle E, ‘The method and role of comparative law’ (2009) 8(3) WUGSLR 451

in public criminology’ (2013) 10(3) EJC 260

-- ‘Multi-centred governance and circuits of power in liberal modes of security’ (2016)
17(3-4) GC 240

30(4) OJLS 725

Edwards JR and Simester AP, ’Wrongfulness and Prohibitions’ (2014) 8(1) CLP 171

Edwards P, ‘Britain’s New Counter Terrorism Legislation Will Undermine the Rule of
Law Even Further’ (Conversation.com, 29 Oct 2018)
<http://theconversation.com/britains-new-counter-terrorism-legislation-will-
undermine-the-rule-of-law-even-further-102871> accessed 15 May 2020

Elliot M and Thomas R, Public Law (OUP 2011)

-- Public Law (2nd edn, OUP 2014)

Elliott C and Quinn F, English Legal System (13th edn, Pearson Essex 2012)

Emmerson B, Ashworth A and Macdonald A (eds), Human Rights and Criminal Justice (3rd edn, Sweet & Maxwell 2012)


Endicott T, ‘The Impossibility of the Rule of Law’ (1999) 19 OJLS 1

Ericson R and Haggerty K, 'Policing the risk society' (Oxford University Press 1997)

Ericson RV, Crime in an Insecure World (Polity Press 2007)

Erlenbusch V, ‘How (not) to Study Terrorism’ (2014) 14(4) CRISPP 470

Eubank WL and Weinberg LB, ‘Does Democracy Encourage Terrorism’ (1994) 6(4) TPV 417

Evans M, ‘Policy Transfer in Critical Perspective’ (2009) 30 PS 243


Fan Mingqiang, Terrorism in the perspective of sociology (社会学视野中的恐怖主义) (People's Liberation Army Press 2005)


Feinberg J, Harm to Others (Oxford University Press on Demand 1984)


-- ‘Proactive Counter-Terrorism Strategies in Conflict with Human Rights’ (2008) 22(3) IRLCT 259


-- ‘Preventative anti-terrorist strategies in the UK and ECHR: Control Orders, TPIMs and the role of technology’ (2011) 25(3) IRLCT 129


Fletcher GP, ‘The Indefinable Concept of Terrorism’ (2006) 4 JICJ 894

Flink A, Conducting A Research Literature Review: From Internet to Paper (Sage 2010)


Forte DF, ‘Terror and Terrorism: There is a Difference’ (1986) 13 ONULR 39


Friedman LM, ‘The Law and Society Movement’ (1986) 38(3) SLR 775


Fu Liqing, ‘Study on the certainty and generality of wording of criminal Law: From the perspective of Criminal Legislation technology(论刑法用语的明确性与概括性——从刑事立法技术角度切入)’ (2013) 2 Journal of Northwest University of Political Science and Law 93


Galli F and Weyembergh A, *EU Counterterrorism Offences* (de l'Université de Bruxelles 2012)


Gani M and Mathew P (eds), *Fresh Perspectives on the War on Terror* (ANU E-Press 2008)


Gearty C, ‘Rethinking civil liberties in a counter-terrorism world’ (2007) 2 EHRLR 111


Gillian and Quinton v UK (2010) (Application no. 4158/05)

Glendon MA, Carozza P and Picker C, *Comparative Legal Traditions: Text, Materials and Cases on Western Law (American casebook series)* (3rd edn, West Academic


Golumbic MC, Fighting Terror Online (Springer 2008)

Goodman MD and Brenner SW, ‘The emerging consensus on criminal conduct in cyberspace’ (2002) 10(2) IJLIT 139

Goold BJ and Lazarus L (eds), Security and Human Rights (Bloomsbury Publishing 2019)


-- ‘Comparative law as the study of transplants and receptions’ in M Reimann and R Zimmermann (eds) Oxford Handbook of Comparative Law (Oxford University Press 2006)
Green A, 'The Quest for a Satisfactory Definition of Terrorism: R v Gul' (2014) 77 MLR 780


Gul [2012] EWCA Crim 280


Guo Zhilong, ‘The Situation of Preventive Criminalization in China: From the perspective of comparison between terrorism and cybercrime(预防性犯罪化的中国境域——以恐怖主义与网络犯罪的对照为视角)’ (2017) 2 Legal Science


Han Ze, ‘Research on Preventive Criminal Legislation of Counter-terrorism(预防性反恐刑事立法研究)’ (Master thesis, HeiLongjiang University 2019)

Hardy K and Williams G, ‘What is “Terrorism”?: Assessing Domestic Legal Definitions’ (2011) 16 UCLAJILFA 77

-- ‘What is ‘Cyberterrorism”? Computer and Internet Technology in Legal Definitions of Terrorism’ in TM Chen, L Jarvis and S Macdonald(eds), Cyberterrorism: Understanding, Assessment, and Response (Springer Science and Business Media 2014)

Harris P, ‘Curriculum Development in Legal studies’ (1986) 20 LT110

Hart HLA, Punishment and responsibility: Essays in the philosophy of law (Oxford University Press 2008)


Hayek FV, The Road to serfdom (University of Chicago Press 1994)

HC Deb 22 February 2005, vol 431, col 40
HC Deb 22 February 2005, vol 431, col 44
HC Deb 22 February 2005, vol 431, col 51
HC Deb 26 Oct 2005, col 344
HC Deb 8th July 2010, vol 513, col 29
HC Deb 9 Nov 2005, vol 439, col 429
HC Deb 9 November 2005,vol 439, col 430
HC Debate 14 Dec 1999, vol 341, col 156
HC Standing Committee D 18 Jan 2000, col 56


-- ‘The expansion and limitation of preventive criminal law(预防刑法的扩张及其限度)’ (2017) 4 Legal Research


Herring J, Criminal Law Text, Cases, and Materials (5th edn, Oxford University Press


HL Deb 15 May 2000, vol 613, cols 751-755

HL Deb 16 May 2000, vol 613, col 230

HL Deb 16 may 2000, vol 613, col 252.

HL Deb 17 January 2006, vol 677, col 583

HL Deb 5 Dec 2005, vol 676, col 435

HL Deb 5 Dec 2005, vol 676, col 458

HL Deb 7 December 2005, vol 676, col 716

HL Deb 8 July 2008, vol 703, col 647

Hodgson J and Tadros V, ‘How to Make a Terrorist Out of Nothing’(2009) 72 MLR 984

-- ‘The Impossibility of Defining Terrorism’(2013) 16(3)NCLR 494

Hoecke MV, ‘Methodology of comparative legal research’ (2015) 12 (3) LM 1


Home office, *Countering International Terrorism: The United Kingdom’s Strategy* (Cm 6888, 2006)

-- *Privy Council Review of Intercept as Evidence: Report to the Prime Minister and the Home Secretary* (Cm 7324, 2008)

-- *Pursue, Prevent, Protect, Prepare: The United Kingdom’s Strategy for Countering International Terrorism* (Cm 7547, 2009)


-- Pursue Prevent Protect Prepare: The United Kingdom’s Strategy for Countering International Terrorism (Cm 7833, 2010)

-- CONTEST: The United Kingdom’s strategy for Countering International Terrorism: Annual Report 2011 (Cm 8123, 2011)

-- Prevent strategy (Cm 8092, 2011)

-- Review of Counter-Terrorism and Security Powers (Cm 8004, 2011)


-- CONTEST: The United Kingdom’s Strategy for Countering Terrorism (Cm 8583, 2013)


-- CONTEST: The United Kingdom’s Strategy for Countering Terrorism (Cm 8848, 2014)

-- Intercept as Evidence (Cm 8989, 2014)

-- CONTEST: The United Kingdom’s Strategy for Countering Terrorism (Cm 9048, 2015)


-- The Government Response to the Report by David Anderson Q.C. on Terrorism Prevention and Investigation Measures in 2014 (Cm 9041, 2015)

-- CONTEST, the United Kingdom’s Strategy for Countering Terrorism: Annual Report for 2015 (Cm 9310, 2016)

-- The UK’s Counter-terrorism Strategy (CONTEST)2018 (Cm 9608, 2018)


Horder J, ‘Harmless Wrongdoing and the Anticipatory Perspective on Criminalisation’ in GR Sullivan, I Dennis (eds), Seeking Security: Pre-empting the Commission of Criminal Harms (Hart Publishing 2012)

-- Ashworth’s Principles of Criminal Law (9th edn, Oxford University Press 2019)

Horne A, The Use of Intercept Evidence in Terrorism Cases Standard Note:

Hou Yanfang, ‘Study on Criminal legal response to Cyberterrorism Crime in China (论我国网络恐怖活动犯罪的刑法规制)’ (2016) 3 Shandong Social Sciences

House of Commons Select Committee on Procedure (HC 588-1, 1977)

House of Commons Standing Order 152B

House of Commons, Post-Legislative Scrutiny: The Government’s Approach (Cm 7320, 2008)

House of Lords Select Committee on the Constitution, Fast track legislation: Constitutional Implications and Safeguards (HL 116 2008-9)

House of Lords Select Committee, First Report on the Constitution (HL 11, 2001)


Hu Xuexiang, 'Improving the Legislative Structure on Punishment', (1996) 2 Modern Law Science 124


Hua J and Bapna S, ‘How Can We Deter Cyberterrorism?’ (2012) 21(2)ISJGP 102


Huang Taiyun and Teng Wei (eds), A Practical Guide and Interpretation of the Criminal Law of the PRC (中华人民共和国刑法释义与适用指南) (The Red Flag Press 1997)

Huang v Secretary of State for the Home Department [2007] UKHL 11


-- ‘China: Ratify Key International Human Rights Treaty’(noting that, “although China has signed the International Covenant on Civil and Political Rights, another important international document regarding the protection of human rights, the country has not yet ratified the treaty”) (Human Rights Watch, 8 Oct 2013)<https://www.hrw.org/news/2013/10/08/china-ratify-key-international-human-rights-treaty> accessed 28 Sep 2020


Hunt A, ‘Criminal Prohibitions on Direct and Indirect Encouragement of Terrorism’ (2007) CLR 441

Husa J, ‘Farewell to Functionalism or Methodological Tolerance?’ (2003) 67(3)RZFAIP 419


-- Overcriminalization: The Limits of the Criminal Law(Oxford University Press 2008)

-- The Philosophy of Criminal Law (Oxford University Press 2010)

Husak DN, ‘Guns and Drugs: Case Studies on the Principled Limits of the Criminal Sanction’(2004) 23(5)LP 437

-- and Duncan N, ‘Defining and Describing What We Do: Doctrinal Legal Research’ (2012) 17(1) DLR 83


Jarvis L and Macdonald S, ‘Locating Cyberterrorism: How Terrorism Researchers Use and View the Cyber Lexicon’ (2014) 8(2)PT 52

-- ‘Responding to Cyberterrorism: Options and Avenues’ (2015) 16 GJIA134

-- ‘What is Cyberterrorism? Findings From a Survey of Researchers’ (2015) 37(1) TPV 68


-- Eighth Report, Renewal of Control Orders Legislation 2011 (HL 106 HC 838, 2011)


Jiang Huiling, ‘Judicial reform’ in Cai Dingjian and Wang Chenguang (eds), China’s
Journey Towards the Rule of Law—Legal Reform 1978–2008 (Brill 2010)

Jiang Min, ‘Authoritarian Informationalism: China’s Approach to Internet Sovereignty’ (2010) 30 SRILA 71


Jiang Zemin, ‘Upholding the great banner of Deng Xiaoping theory to fully push the establishment of socialism with Chinese characteristics into the twenty-first century(高 举邓小平理论的伟大旗帜，把建设有中国特色的社会主义全面推向 21 世纪)’ (1997) 18 Seeking Truth Magazine 3

-- ‘Jiang’s speech in 2001’ People’s Daily (Beijing, 1 Feb 2001)


Jobe v UK [2011] (Application no.48278/09)


-- Counter-Terrorism Policy and Human Rights: Terrorism Bill and Related Matters (HL 75-I, HC 561-I,2005–6,)


Jones T and Newburn T, Policy Transfer and Criminal Justice (Open University Press 2007)


JJ 19


K [2008] EWCA Crim 185, [2008] 3 All ER 526

K v R [2008] EWCA Crim 185

Kaiman J, ‘China cracks down on social media with threat of jail for ‘online
rumours”(*the Guardian*, 10 Sep 2013) <https://www.theguardian.com/world/2013/sep/10/china-social-media-jail-rumours>
accessed 21 September 2019

Kalhan A and others, ‘Colonial continuities: human rights, terrorism, and security laws
in India’ (2006) 20 CJAL 93


Kang Junxin and Yu Wenliang, ‘Legal Response to Cyber Terrorism in the Era of Big
Data(大数据时代网络恐怖主义立法应对)’ (2015) 10 Academic Journal of Zhongzhou 60

Kang Junxin, ‘The Formation and Development of Anti-terrorism Theory in New Era of
Xi Jinping(习近平新时代反恐理论的形成与发展)’ (2018) 5 Research on Law and
Economy 1

Kassa WD, ‘Examining Some of the Raisons d’Etre for the Ethiopian Anti-terrorism
Law’ (2013) 7 (1)MLR 49


Explanatory Factors’ (2005)12 (5) JEPP 764

Kokkinakis v Greece (1993) 17 EHRR 397

http://www.crime-research.org/library/Cyber-terrorism.htm> accessed 13 September
2020;

L Friedman, ‘On Human Rights, the United States and the People’s Republic of China
at Century’s End’ (1998)4 JILS 241

Laborde JP, ‘Countering Terrorism: New International Criminal Law Perspectives’
(132nd International Senior Seminar Visiting Experts’ Papers, United Nations Asia and
Far East Institute for the Prevention of Crime and the Treatment of Offenders (*UNAFEI*,
accessed 20 Nov 2020

343

LaFree G, L Dugan and E Miller, Putting Terrorism in Context: Lessons from the Global Terrorism Database (Routledge 2015)

Lam WWL, China after Deng Xiaoping (John Wiley & Sons 1995)


Laqueur W, A History of Terrorism (Transaction Publishers 2001)

lasiello E, ‘China’s Cyber Initiatives Counter International Pressure’ (2017) 10(1) JSS 1

Laurent M and Choon YJ, ‘A Comparative Examination of Counter-Terrorism Law and Policy’ (2016) 16 JKL91

Lavender & Son Ltd v Minister of Housing [1970] 3 All ER 871


-- ‘Positive Obligations and Criminal Justice: Duties to Protect or Coerce?’ in JV Roberts and L Zedner (eds), Principled Approaches to Criminal Law and Criminal Justice: Essays in Honour of Professor Andrew Ashworth (OUP 2012)


Ledford KF, ‘Formalizing the Rule of Law in Prussia: The Supreme Administrative Court 1876-1914’ (2004) 37 (2)CEH 203

Lee JA, ‘Regulating Blogging and Microblogging in China’ (2012) 91 OLR 609


-- ‘The impossibility of “legal transplants”’ (1997) 4(2) MJECL111

-- ‘John Merryman and Comparative Legal Studies: A Dialogue’ (1999) 27 AJCL 50

Levičev V, ‘The Synthesis of Comparative and Socio-Legal Research as the Essential Prerequisite to Reveal the Interaction of National Legal Systems’ (The Interaction of National Legal Systems: Convergence or Divergence? International Conference of PhD Student and young Researchers, Vilnius, Apr 2013)

Lewis JA, ‘Assessing the risks of cyber terrorism, cyber war and other cyber threats’


-- ‘The Cultural Idiosyncrasy of Penal Populism-The Case of Contemporary China’ (2015) 55 BJC 146


-- ‘Fighting the Three Evils: A Structural Analysis of Counter-Terrorism Legal Architecture in China’ (2019) 33(3)EILR 311


Li Hong, ‘On the Prescriptions on the Offences Concerning Terrorism and Extremism in the PRC’s Criminal Law Amendment IX from the Perspective of Limiting Potential Damage Offense(《刑法修正案(九)》中有关恐怖主义、极端主义犯罪的刑事立法——从如何限缩抽象危险犯的成立范围的立场出发)’ (2015) 6 Journal of Soochow University(Philosophy & Social Science Edition) 84

Li Meixian, ‘China’s Compliance with WTO Requirements Will Improve the Efficiency and Effective Implementation of Environmental Laws in China’ (2004)18 TICLJ 155

Li Q, ‘Democracy, Autocracy, and Expropriation of Foreign Direct Investment’ (2009) 42 (8) CPS 1098


Li Tao, ‘Research on the prevention and control of cyber terrorism crime from the perspective of overall national security (总体国家安全观视角下网络恐怖主义犯罪防控研究)’ (2019) 4 Journal of China Criminal Police College 5

Li Yan, ‘Study of Legal issues of Cyber terrorism crime identification(网络恐怖主义犯罪认定法律问题研究)’ (Master thesis, Lanzhou University 2018)

Li Zhe and Zhang Yi, ‘Comparison of inciting terrorism act in China and the UK’ (2016) 24(5) Journal of the National Prosecutor’s College 49

Li Zhe, ‘China’ in K Roach(ed), Comparative Counter-Terrorism Law (Cambridge University Press 2015)

Liao Zengyun, ‘Basic Principles that Should Be Clearly Adopted in Our Criminal Law’ (1990) 1 Legal Science in China 54


Linz JJ, Totalitarian and authoritarian regimes (Lynne Rienner Publishers 2000)

Liu Renwen, ‘Description and Analysis of China's Anti-terrorism Criminal Legislation’ (中国反恐刑事立法的描述与评析)’ (2013) 4 The Jurist 45


Liu Yanhong, ‘China should stop overcriminalization legislation(我国应当停止犯罪化的刑事立法)’ (2011) 11 Law Science


Liversidge v Anderson [1942] AC 206


Lloyd of Berwick L, Inquiry into Legislation against Terrorism (Cm 3420,1996)

Lord Alton of Liverpool & Others (in the Matter of the People’s Mojahaddeen Organisation of Iran) v Secretary of State for the Home Department, Proscribed Organisations Appeal Committee(POAC), Appeal No: PC/02/2006

Loveland I, Constitutional and Administrative Law (OUP 2012)

Lu H, Liang B and Taylor M, ‘A Comparative Analysis of Cybercrimes and
Lubman SB, *China’s Legal Reforms* (Oxford University Press 1999)

-- *Bird in a Cage: Legal reform in China after Mao* (Stanford University Press 1999)

-- ‘Looking for Law in China’ (2006) 20 CJAL 1


Lynch A, ‘Control Orders in Australia: A Further Case Study of the Migration of British Counter-Terrorism Law’ (2008) 8 OUCLJ 159

Lynch A, MacDonald E and Williams G (eds), *Law and Liberty in the War on Terror* (The Federation Press 2007)


M v Home Office [1992] 2 WLR 73


MacDonald S, ‘ASBOs and Control Orders: Two Recurring Themes, Two Apparent Contradictions’ (2007) 60(4) PA 601

-- ‘The Unbalanced Imagery of Anti-terrorism Policy’ (2009) 18 CJLPP 519

-- ‘Why We should Abandon the Balance Metaphor: a New Approach to Counterterrorism Policy’ (2009) 15 ILSA JICL 95


-- ‘Social Media, Terrorism Content Prohibitions and the rule of law’ (2019) PEGWU 1


-- Jarvis L and Lavis SM, ‘Cyberterrorism Today? Findings From a Follow-on Survey of Researchers’ (2019) 37(1)SCT 1

-- and Carlile L, ‘Disrupting terrorist activity: What are the limits to criminal methods of disruption?’ in SS Juss (eds), Beyond Human Rights and the War on Terror (Routledge Research in Human Rights Law 2019)

-- and Lorenzo-Dus N, Purposive and Performative Persuasion: The Linguistic Basis for Criminalising the (Direct and Indirect) Encouragement of Terrorism (OUP 2019)


Manap NA and Tehrani PM, ‘Cyber Terrorism: Issues in Its Interpretation and Enforcement’ (2012) 2(3) IJIEE 409

Marchand SA, ‘An Ambiguous Response to a Real Threat: Criminalizing the Glorification of Terrorism in Britain’ (2010) 42 GWILR123


Mathews AS, Freedom, State Security and the Rule of law (Sweet & Maxwell 1988)


Mayali L and Yoo J, ‘A Comparative Examination of Counter-Terrorism Law and Policy’ (2016) 16 JKL 91

McConville M and Chui WH (eds), Research Methods for Law (Edinburgh University Press 2007)


-- ‘Putting the ‘Cyber’ into Cyberterrorism: Re-reading Technological Risk in a Hyperconnected World’ in TM Chen and others (eds), Cyberterrorism: Understanding, Assessment, and Response (Springer Science+Business Media 2014)


Mei Chuanqiang and Li Jie, ‘The Review of Anti-terrorism Criminal Legislation in China (我国反恐刑法立法的预防性面向“检视”’) (2018) 1 The Legal Science 48

Mei Chuanqiang, ‘Review and improvement of China’s anti-terrorism criminal legislation: evaluation of terrorism-related offences in Amendment(IX) (我国反恐刑事立法的检讨与完善--兼评〈刑法修正案(九)〉相关涉恐条款)’ (2016) 1 Modern Law


Merkur Island Shipping Corporation v Laughton [1983] 2 AC 570 (Lord Diplock)

Michael S, ‘Cyber Terrorism: A Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Games?’ (2006) 46(4–5) CLSC 223

Middleton B, ‘Rebalancing, Reviewing or Rebranding the Treatment of terrorist Suspects: The Counter- Terrorism Review 2011’ (2011) 75(3) JCL 225


Mill JS, On Liberty (1859)

Miller C, ‘Is it Possible and Preferable to Negotiate with Terrorists?’ (2011) 11(1)DS 145


Morris C and Murphy C, *Getting a PhD in Law* (Hart Publishing 2011)


* -- EU Counter- Terrorism Law: Pre-Emption and the Rule of Law* (Hart Publishing 2012)

Mythen G and Walklate S, ‘Criminology and Terrorism’ (2006) 46(3)BJC 379


Nelken D, *Comparing Legal Cultures* (Dartmouth 1997)

* -- Comparative Criminal Justice: Making Sense of Difference* (Sage Publications 2010)

* -- Comparative Criminal Justice and Globalisation* (Ashgate 2011)


* -- and J Feest (eds), *Adapting Legal Cultures* (Hart Publishing 2001)


Neuberger L, the president of the UK Supreme Court, ‘Justice – Tom Sargant Memorial


Ni Chunle, Special Procedures for Terrorism Crimes(恐怖主义犯罪特别诉讼程序)(Masses Publishing 2013)


Omand D, Securing the State (Hurst & Co Publishers 2010)

Ong YN, ‘International Responses to Terrorism: The Limits and Possibilities of Legal Control of Terrorism by Regional Arrangement with Particular Reference to Asean’ (2002) IDSS


-- ‘Developing Comparative Law’ in E Örücü and D Nelken (eds), Comparative Law: A Handbook (Hart 2007)


Osiatynski W, Paradoxes of Constitutional Borrowing’ (2003) 1(2) IJCL 244

Osman v United Kingdom [1998] EHRR 101

Oyen E, *Comparative Methodology Theory and Practice in International Social Research* (SAGE Publisher 1990)


Pan Dongmei and Gao Mingxuan, ‘Formation of the Basic Principles in the Modern Chinese Criminal Law’ (2016) 10 Journal of Siberian Federal University (Humanities & Social Sciences) 2465

Pan Guanyuan and Zhang Debiao, *Strategy on Anti-Cyberterrorism: How to deal with Cyberterrorism (网络反恐大策略: 如何应对网络恐怖主义)* (Current Affairs Publishing Press 2016)


Pape RA, ‘The Strategic Logic of Suicide Terrorism’ (2003) 97 (3) APSR 343


Parmer A, ‘Stop and Search in London: Counter-Terrorist or Counter-Productive?’ (2011) 21 (4) PS 369


--- *China’s Long March Toward Rule of Law* (CUP 2002)

-- ‘The X-Files: Past and Present Portrayals of China’s Alien "Legal System"’ (2003) 2 WUGSLR 37


-- *China Modernizes: Threat to the West or Model for the Rest?* (OUP 2008)

People net, ‘Kunming Handled 224 Administrative Cases in relation to the CTL and 23 Individuals were Detained’ (<http://yn.people.com.cn/n2/2018/0823/c378439-31966460.html> accessed 15 June 2020)

Petzsche A and Melia MC, ‘Speaking of Terrorism and Terrorist Speech: Defining the Limits of Terrorist Speech Offences’ in G Lennon, C King and C McCartney (ed), Counter-Terrorism, Constitutionalism and Miscarriages of Justice: A Festschrift for Professor Clive Walker (Hart 2019)


-- Research on Legislations against Cyber-Terrorism(防控网络恐怖活动立法研究) (Law Press 2017)

Piazza JA, ‘Regime age and terrorism: Are New Democracies Prone to Terrorism?’ (2013) 39(2) II 246

Pitaksantayothin J, ‘Cyber Terrorism Laws in the United States, the United Kingdom and Thailand: A Comparative Study’ (2014) 32(2)CLJ 169

Pokalova E, ‘Authoritarian Regimes against Terrorism: Lessons from China’ (2013) 6 (2) CST 279


Pollitt MM, ‘Cyberterrorism: Fact or Fancy’ (the proceedings of the 20th National Information Systems security Conference, Baltimore 1997)


Posner RA, ‘The Present Situation in Legal Scholarship’ (1980) 90 YLJ 1113


Prasad K, ‘Cyberterrorism: Addressing the Challenges for Establishing an International Legal Framework’ (3rd Australian Counter Terrorism Conference, Perth, 3rd -5th December 2012)


Rutland J, ‘Regime type and Cyberterrorism’ (Master thesis, Augusta University 2019)


accessed 3 September 2020


-- Terrorism Prevention and Investigation Measures in 2013 Grahame Allen and Noel Dempsey, Terrorism in Great Britain: The Statistics (House of Commons Library 2018)


Qin Guanying, Research on Terrorism Crime from the Perspective of Non-traditional Security(非传统安全视域下的恐怖主义犯罪研究) (Law Press 2018)

R (Corner House Research and another) v Director of the Serious Fraud Office [2008] EWHC 714 (Lord Justice Moses)

R (Corner House Research) v Director of the Serious Fraud Office [2008] UKHL 60

R (Jackson) v Attorney-General [2006] 1 AC 262 (Lord Hope)

R v Davison (Unreported, Newcastle Crown Court, Milford J, 14 May 2010)
R v Gul [2013] UKSC 64, [2013] 3 WLR 1207
R v Home Secretary, ex parte Venables [1998] AC 407
R v K [2001] UKHL 41
R v R [1991] 2 WLR 1065

Rainer JM, *Introduction to Comparative Law* (Manz 2010)


-- *The Insecurity State: Vulnerable Autonomy and the Rights to Security in the Criminal Law* (OUP 2012)

-- ‘Democratic Limits to Preventive Criminal Law’ in A Ashworth, L Zedner and P Tomlin (eds), *Prevention and the Limits of the Criminal Law* (OUP 2013)


Razak AA, ‘Understanding legal research’ (2009) 4 ID 21

Reitz JC, ‘How to Do Comparative Law’ (1998) 46(4) AJCL 617

Reuters, ‘China launched a special action to eradicate audio and video of violent and terrorism on the Internet’ (Reuter, 20 June 2014) <https://www.reuters.com/article/china-anti-terror-av-material-idCNKBSOEV10520140620> accessed 5 Dec 2020


Reynolds v Times Newspapers [2001] 2 AC 127


Ridge v Baldwin [1964] AC 40

Riles A, ‘Comparative Law and Socio-legal Studies’ in M Reimann and R
Zimmermann (eds), *The Oxford Handbook of Comparative Law* (Oxford University Press 2006)


-- ‘Must We Trade Rights for Security? The Choice between Smart, Harsh or Proportionate Security Strategies in Canada and Britain’ (2006) 27(5) CLR 2151


-- ‘The Case for Defining Terrorism with Restraint and without Reference to Political or Religious Motive’ in A Lynch, E MacDonald and G Williams (eds), *Law and Liberty in the War on Terror* (The Federation Press 2007)


-- ‘Defining Terrorism: The Need for a Restrained Definition’ in N LaViolate and C Forcese (eds), *The Human Rights of Anti-Terrorism* (Irwin Law 2008)

-- ‘Sentencing Terrorists’ (2011) 57(1) CLQ 1

-- *The 9/11 Effect: Comparative Counter-Terrorism* (Cambridge University 2011)


-- ‘Terrorism’ in M Dubber and T Hornle (eds), *Oxford Handbook of Criminal Law* (OUP 2014)

-- ‘Comparative Counter Terrorism Law Comes of Age’ in K Roach (ed), *Comparative Counter-Terrorism Law* (Cambridge University 2015)


Robinson PH, ‘Rule of Conduct and Principles of Adjudication’ (1990) 57 UCLR 729


Rollins J and Wilson C, ‘Terrorist capabilities for Cyber Attack: Overview and Policy Issues’ in EV Linden, Focus on Terrorism(Nova Publisher 2007) 43


Rossiter CL, Constitutional Dictatorship (Harcourt 1948)


Rutland J, ‘Regime type and Cyberterrorism’ (Master thesis, Augusta University 2019)


S Lubman, China’s Legal Reforms (Oxford University Press 1996)


Saich T, Governance and Politics of China (Palgrave 2001) 126


Samina Malik (2008) EWCA Crim 1450


-- ‘Speaking of Terror: Criminalising Incitement to Violence’ (2005) 28 UNSWLJ 868


-- Defining Terrorism in International Law (Oxford University 2006)

-- ‘The Curious Element of Motive in Definitions of Terrorism: Essential Ingredient or Criminalising Thought?’ in A Lynch, E MacDonald and G Williams (eds), Law and Liberty in the War on Terror (The Federation Press 2007)

-- ‘Criminality and Terrorism’ (2010) 106 (10)SLSLSRP 1


-- ‘Submission to Council of Australian Government (COAG)’ (2012) 6 RCTL

-- ‘Criminality and Terrorism’ in AM Salinas de Friás, KLH Samuel and ND White(eds),
Counter-Terrorism, The Security Imperative and The Rule of Law (Oxford University Press 2012)


-- ‘The international standardization of national security law’ (2010) 4(2) JNSLP 438

Schlesinger RB, ‘The Role of the “Basic Course” in the Teaching of Foreign and Comparative law’ (1971) 19 AJCL 616

Schmid AP, ‘Terrorism and Democracy’ (1992) 4 (4) TPV 14

-- ‘Terrorism: The Definitional Problem’ (2004) 36 (2) CWRJIL 375

-- ‘Frameworks for Conceptualising Terrorism’ (2004) 16(2) TPV 197


Schmittho M, ‘The Science of Comparative Law’ (1939) 7 CLJ 94


Scoppola v Italy (no 2) [GC], no. 10249/03, 17 September 2009


Secretary of State for the Home Department v AP [2010] UKSC 24

Secretary of State for the Home Department v E [2007] EWHC 233 (Admin)

Secretary of State for the Home Department v J.J. and others [2006] EWHC 1623 (Admin)

Secretary of State for the Home Department v Lord Alton of Liverpool and others [2008] EWCA Civ 443, [2008] 1 WLR 2341
Secretory of State, *Justice and Security Green Paper: Response to Consultation from Special Advocates* (Cm 8194, 2011)


Sheldrake v Director of Public Prosecutions; Attorney General's Reference (No 4 of 2002) [2004] UKHL 43


Shishi Li, then director of the Legal Work Committee of the Standing Committee of the National People’s Congress, ‘gave an explanation on the draft of the Criminal Law Amendment (IX)’ (<http://www.gov.cn/xinwen/2014-10/28/content_2771624.htm>) accessed 20 Oct 2020


Sieb P and Janbek DM, *Global Terrorism and the New Media* (Routledge 2011)


Simeon JC, ‘The Evolving Common Law Jurisprudence Combatting the Threat of Terrorism in the United Kingdom, United States, and Canada’ (2019) 8(1)L 5


-- ‘Prophylactic Crimes’ in GR Sullivan and I Dennis (eds), *Seeking Security: Pre-Empting the Commission of Criminal Harms* (Hart Publishing 2012)

-- and Hirsch AV, ‘Remote Harms and Non-constitutive Crimes’ (2009) 28 (1) CJE 89


Singhal AK and Malik I, ‘Doctrinal and Socio-legal Methods of Research: Merits and Demerits’ (2012) 2(7) ERJ 252


Sliedregt EV, ‘European Approaches to Fighting Terrorism’ (2010) 20 DJCIL 413
Smith and Grady v UK (1999) 29 EHRR 493

Smith ATH, ‘Dicey and Civil Liberties: Comment’ (1985) PL 608


Sohail Anjum Qureshi [2008] EWCA Crim 1054


SSHD v AF, AN and AE [2009] UKHL 28

SSHD v Daley [2001] UKHL 26


Steyn J, ‘Democracy, the Rule of Law and the Role of Judges’ (2006) EHRLR 1


Su Li, ‘Governance of International Cyber Terrorism and Its Enlightenment to China(国 际网络恐怖主义的治理及其对中国的启示)’ (Master Thesis, Xiangtan University 2012)


Su Shaozhi, ‘Theory and Practice of the CCP on Reforming the Political System in Deng Xiaoping Era( 邓小平时代 中国 政治 体 制 改 革的 理论和 实践 )’ (1999) 66(3)Contemporary China Studies

Sullivan GR and Dennis I (eds), Seeking Security: Pre-empting the Commission of Criminal Harms (Hart Publishing 2012)

Sun Junjie, ‘The Development, Prevention and Control of Terrorism Crimes in the Internet Age(网络时代下 恐怖主义 犯罪的 发展和防 控)’ (2016) 4 Journal of Heilongjiang Administrative Cadre College of Politics And Law 26
Sun Pinjie, ‘Research on the problems and Countermeasures of technical intelligence in anti-terrorism work (技术情报在反恐工作中存在的难题及对策研究)’ (2019) 3 Journal of Intelligence 26


Sunday Times v UK (1979) 2 EHRR 245


SW and CR v UK (1995) 21 EHRR 363

SW and CR v UK [1996] 21 EHRR 363


Tadros V, ‘Justice and Terrorism’ (2007) 10 (4) NCLR 658

-- ‘Rethinking the presumption of innocence’ (2007) 1(2) CLP 193

-- ‘Crimes and Security’ (2008) 71(6)MLR 940


-- and Hodgson J, ‘How to Make a Terrorist Out of Nothing’ (2009) 72(6) MLR 984

Tafoya WL, ‘Cyber terror’ (2011) 80 (1) FBILEB

Talihärm AM, ‘Cyberterrorism: In Theory or in Practice?’ (2010) 3(2) DATR 59


Tang Lan, ‘Aspects of cyber terrorism(网络恐怖主义面面观)’ (2003) 7 International information


law-defense-offense> accessed 8 November 2020

Tehrani PM, *Cyberterrorism: The Legal and Enforcement Issues* (World scientific press 2017)

Tehrani PM, Manap NA and Taji H, 'Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime' (2013) 29 CLSR 207


The Council of Europe, *Cyberterrorism: The Use of The Internet for Terrorist Purposes* (Council of Europe Publishing 2008)


The Supreme People's Court published 3 model cases regarding Fabricated Terror Threat' (People net, 29 Sep 2013)<http://legal.people.com.cn/n/2013/0929/c188502-23074503.html> accessed 13 Nov 2020


Theohary CA and Rollins J, Terrorist Use of the Internet: Information Operations in Cyberspace (DIANE Publishing 2011)


-- The Death Penalty in Contemporary China (Springer 2012)

-- and Nesossi E, ‘Control By Law’ in J Golley, L Jaivin and L Tomba (eds), Control: China Story Yearbook 2016 (ANU Press 2017)


UN Commission on Human Rights, ‘General Comment No. 29: States of Emergency (Article 4)’ (31 August 2001) UN Doc CCPR/C/21/Rev.1/Add.11


UN General Assembly, Resolution 55/63 (4 Dec 2000), UN Doc A/RES/55/63

-- Resolution 56/121 (19 Dec 2001), UN Doc A/RES/56/121

-- ‘Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism’ (16 August 2006) UN Doc A/61/267

UN Security Council, Resolution 1373 (28 September 2001) UN Doc S/RES/1373

-- Resolution 1624 (14 Sep 2005), UN Doc S/RES/1624

-- Res 2178 (24 Sep 2014) UN Doc S/Res/2178


UN Treaty Series, vol. 2178


Usman Kham and others [2013] EWCA Crim 468


Verton D, Black ice: The invisible threat of cyber terrorism(McGraw Osborne Media 2003)

Vicziany M, ‘State Responses to Islamic Terrorism in Western China and Their Impact on South Asia’ (2010) 12(2) CSA 243


Wagstaff RH, Terror detentions and Rule of law: US and UK perspective (Oxford University Press 2014)


-- ‘Safety and Security’ (2006) 85 NLR 454


-- ‘Clamping Down on Terrorism in the United Kingdom’ (2006) 4 JICJ 1147

-- ‘Intelligence and Anti-Terrorism Legislation in the United Kingdom’ (2005) 44 CLSC 387

-- ‘Cyber-terrorism: Legal principle and the law in the United Kingdom’ (2006) 110(3) PSLR 625
-- ‘Keeping Control of Terrorists Without Losing Control of Constitutionalism’ (2007) 59 SLR 1395

-- 'The Legal Definition of "Terrorism" in United Kingdom Law and Beyond' (2007) PL 331

-- ‘Terrorism: Terrorism Act 2000, s.1 and 58--Possession of Terrorist Documents’ (2008) CLR 72

-- ‘Neighbor Terrorism and the All-Risk Policing of Terrorism’ (2009) 3 JNSLP 121

-- ‘Prosecuting Terrorism: The Old Bailey versus Belmarsh’(2009) 79 AC 21


-- 'The Threat of Terrorism and the Fate of Control Orders' (2010) 3PL 4

-- Terrorism and the Law (Oxford University Press 2011)


-- ‘Terrorism Prosecution in the United Kingdom: Lessons in the Manipulation of Criminalisation and Due Process’ in F Aolain and O Gross (eds), Guantamano and Beyond: Exceptional Courts and Military Commissions in Comparative and Policy Perspective (Cambridge University Press 2013)

-- ‘The Reshaping of Control Orders in the United Kingdom: Time for A Fairer Go, Australia’ (2013) 37 UMLR 143


-- and Conway M, ‘Online Terrorism and Online laws’ (2015) 8(2) DAC 156


Wang AL, ‘Regulating Domestic Carbon Outsourcing: The Case of China and Climate Change’ (2014) 61 UCLALR 2018

Wang Bingzhang, Shenzhen intermediate people’s Court of Guangdong Province(2003)深中法刑一初字第 41 号(Shen Zhong Fa Xing Yi Chu Zi No.41) <http://china.findlaw.cn/data/gsflgw_4397/1/30896.html> accessed 21 May 2020

Wang Chenguang, ‘From the Rule of Man to the Rule of Law’ in Cai Dingjian and Wang Chenguang (eds), China’s Journey Towards the Rule of Law—Legal Reform 1978–2008 (Brill 2010)


Wang Hanbin, ‘Explanations on the Dra Revision of the Criminal Law of the PRC’ in Huang Taiyun and Teng Wei (eds), A Practical Guide and Interpretation of the Criminal


Wang Mingjin, ‘Characteristics of Post Cold War Terrorism and International Cooperation (后冷战时期恐怖主义的特点与国际反恐合作)’ 2004 1 International Forum 14


Wang Xiumei and Zhao Yuan, ‘A Study of Contemporary Counter-Terrorism Criminal Policies in China(当代中国反恐刑事政策研究)’ (2016) 3 Journal of Beijing Normal University (Social Sciences) 138

Wang Yan, Chinese Legal Reform: The Case of Foreign Investment Law (Routledge 2002)


Wang Zhixiang (ed), Interpretation and Analysis of the Amendment (VIII) to the Criminal Code (Chinese People’s Public Security University Press 2012)


Watson A, Legal Transplants: An Approach to Comparative Law (2nd ed, University of Georgia 1993)

Wayne M, ‘Inside China’s War on Terrorism’ (2009)18(59)JCC 249


Weimann G, ‘Cyberterrorism, How Real is the Threat?’ (2004) 119 SRUSIP 1


-- ‘Cyberterrorism: The Sum of all Fears?’ (2005) 28(2) SCT 129


Wiratraman HP, ‘The Challenges of Teaching Comparative Law and Socio-Legal Studies at Indonesia’s Law Schools’ (2019) 14 AJCL 229


Xia Yixue, Lan Yuexin and Wang Shacheng, ‘Risk analysis and Prevention Countermeasures of Cyberterrorism in big data environment(大数据环境下网络恐怖主义风险分析与防范对策研究)’ (2017) 11 Journal of Intelligence16

Xiang Zhun, ‘Study on the Strict Criminalization of the Crime of Terrorist Activities——Based on the Criminal Law Amendment (IX)((对恐怖活动犯罪现象的严刑化规制研究——以<刑法修正案(九)>为基点)’) (2016) 2 Xinjiang Social Science Forum 37

Xiao Shengyun, ‘Research on Cyber Terrorism Crime’ (Master Thesis, Graduate School of Chinese Academy of Social Sciences 2018)


Xie Bo, ‘Investigation on the Legalization of Criminal Procedure of Terrorism in China(我国恐怖主义犯罪诉讼程序法治化问题探讨)’ (2016)1 Journal of Public Security University of China


-- ‘The Communist Party of China Central Committee Decided to Adjust the Administration of People’s Armed Police (中共中央决定调整中国人民武装警察部队领导指挥体制’ (Xinhua, 27 December 2017) <http://www.xinhuanet.com/politics/2017-12/27/c_1122175909.htm> accessed 20 Oct 2020


Xu Guimin, ‘Study on the Boundary of criminal liability of cyberterrorism in China(论中国网络恐怖主义犯罪边的边际)’ (2018) 2 Social Science in Heilongjiang 27

Xu Shanghao, ‘Research on the Designation Process of Terrorism Organisations and Individuals (恐怖活动组织与人员的认定程序研究)’ (2016) 3 Shandong Social Sciences 112


Yang Jiaojiao, ‘The First Case Concerning the Counter-Terrorism Law in Jinan(济南涉 反 恐 法 第 一 案)’ (Legal Daily, 26 Apr 2016)<http://www.legaldaily.com.cn/index/content/2016-04/26/content 6602490.htm?node=20908.> accessed 13 May 2020


Yannakogeorgos P, ‘Rethinking the threat of cyberterrorism’ in T Chen, L Jarvis and S Macdonald (eds), Cyberterrorism: Understanding, Assessment, and Response(Springer 2014)

Yates J, ‘Metropolitan Police Service Assistant Commissioner Specialist Operations

Young R, ‘Defining Terrorism: The Evolution of Terrorism as a Legal Concept in International Law and Its Influence on Definitions in Domestic Legislation’ (2006) 29(1) BCICLR23


Yu Li, ‘Theoretical discussion on National Cybersecurity’ (关于互联网国家安全的理论探讨) (2018) 3 International Observation 16


Yu Xiaofeng, Pan Yihe and Wang Jiangli, Introduction to Non-Traditional Security (非传统安全概论) (Zhejiang People’s Press 2006)


Yu Xuede, ‘Rule of law or rule by law, governing the people or governing the power? a summary of debates on the issue of governing the state according to law 法制还是法治, 治民还是治权:关于依法治国问题讨论观点综述’ (1997) 12 The Front Line 26

Yu Zhigang and Guo Zhilong, ‘Cyberterrorism Crimes and Responses from Law in China: Analysis and Reflection Based on 100 Random Cases’ (网络恐怖活动犯罪与中国法律应对—基于100个随机案例的思考) (2015) 55(1) Journal of Henan University Social Science


Zafar Butt, Iqbal, Raja and Malik [2008] EWCA Crim 184


-- ‘Neither safe nor sound? The Perils and Possibilities of risk’ (2006) 48(3) CJCCJ 423
-- ‘Pre-Crime and Post-Criminology?’ (2007) 11 TC 261

-- ‘Preventive justice or pre-punishment? The case of control orders’ (2007) 60(1) CLP174

-- Security (Routledge 2009)

-- ‘Fixing the future? The pre-emptive turn in criminal justice’ in B McSherry, A Norrie and S Bronitt (eds), Regulating Deviance: The Redirection of Criminalisation and the Futures of Criminal Law (Hart Publishing 2009)

-- ‘Terrorizing Criminal Law’ (2014) 8(1) CLP 99


Zhai Xiufeng, ‘The mobilization characteristics and dilemma of Cyberterrorism Countermeasures(网络恐怖主义的动员特征及应对困境)’ (2017) 39 Modern communication (Journal of Communication University of China) 160


Zhang Hong, ‘The Impact of Post Cold War Big Power Relations on Terrorism (冷战后大国关系对恐怖主义的影响)’ (2004) 25 Renmin University of China

Zhang Jiaming, ‘Legislative governance of cyber terrorism in the era of big data(大数据时代网络恐怖主义的立法治理)’ (2018) 1 South China Sea Law 81


Zhang Mina, ‘Study On Legal Issues Related to Cyber Terrorism and Legislation Suggestions in China(论网络恐怖主义相关法律问题及我国的立法建议)’ (2016) 31(2)Graduate Law Review 137


-- 'The Study on Terrorism-related offences in Criminal Law Amendment(IX),(论<刑法修正案(九) 关于恐怖犯罪的规定)‘ (2016) 1 Modern Law


Zhang Xun, ‘Research on the Crime of Picking Quarrels and Provoking Troubles, from the Perspective of Pocket Crime (口袋罪视域下的寻衅滋事罪研究)’ (2013) 3 Politics and Law


Zhao Bingzhi, Thematic Research on the Basic Theories of Criminal Law(刑法基本理论专题研究) (Law Press 2005)

-- The Latest Understanding of the Criminal Law Amendment(刑法修正案最新理解适用) (China Legal Publishing Press 2009)

-- Understanding and Application of Amendment (IX) to Criminal Law of the PRC (China Legal Press 2016)

-- and Du Miao, ‘pre-protection of legal interests and weave dense net of anti-terrorism provisions in Criminal Law Amendment(刑法修正案九中法益保护前置织密反恐法网)’ Procuratorial daily (Beijing, 28th Sep 2015)


Zhao Chen, ‘Cyberspace has become a new platform of international counter-terrorism’(China’s Office of Central Space Affairs Commission(中共中央网络和信息化委员会办公室), 14 Jun 2017)< http://www.cac.gov.cn/2017-06/14/c_1121140970.htm> accessed 20 June 2020

Zhao Suisheng, ‘Political Liberalization without Democratization: Pan Wei’s Proposal for Political Reform’ in Suisheng Zhao(ed), Debating Political Reform in China: Rule of Law vs. Democratization(M.E. Sharpe 2006)


Zheng Chengsi, ‘Review Cyber Security legislations in China,(检讨我国信息网络安全


Zhou Guangquan, The Establishment of Positive Outlook on Criminal Legislation in China(积极刑法立法观在中国的确立), (2016) 4 Legal Research 23


Zhou Yongkuan, ‘Review of the Symposium on Administering the State According to Law and Building up a Socialist Country based on the Rule of Law(依法治国,建设社会主义法治国家理论研讨会书评)’ (1997) 2 Rule of Law and Social Development


-- Balancing Security and Liberty: Counter-Terrorism Legislation in Germany and China (Dunker & Humblot 2014)


Zhu Yongbiao and Ren Yan, Research on International Cyberterrorism(国际网络恐怖主义研究)(China Social Sciences Press 2014)

Zhu Yongbiao, Wei Yueyan and Liang Xin, ‘Cyber-terrorism: Trends and Countermeasures(网络恐怖主义的发展趋势与应对现状评析)’ (2016) 18(3)Journal of...
Jiangnan Social University
