Harmonisation and Cybercrime Jurisdiction: Uneasy Bedfellows?

An analysis of the jurisdictional trajectories of the Council of Europe's Cybercrime Convention

Micheál Aaron O' Flynn

School of Law

Queen Mary, University of London

2014

Submitted in partial fulfillment of the requirements
of the Degree of Doctor of Philosophy
Queen Mary, University of London

I, Micheál Aaron O' Flynn, confirm that the research included within this thesis is my own work or that where it has been carried out in collaboration with, or supported by others, that this is duly acknowledged below and my contribution indicated. Previously published material is also acknowledged below.

I attest that I have exercised reasonable care to ensure that the work is original, and does not to the best of my knowledge break any UK law, infringe any third party's copyright or other Intellectual Property Right, or contain any confidential material. I accept that the College has the right to use plagiarism detection software to check the electronic version of the thesis.

I confirm that this thesis has not been previously submitted for the award of a degree by this or any other university. The copyright of this thesis rests with the author and no quotation from it or information derived from it may be published without the prior written consent of the author.

Micheál O' Flynn

23 December 2014.

Details of collaboration and publications:

- Some paragraphs from chapter four, section 4.3 are drawn from a previous publication:
  *O'FLOINN, M., 'It Wasn't All White Light Before *Prism:* Law Enforcement Practices in Gathering Data Abroad, and Proposals for Further Transnational Access at the Council of Europe', *Computer Law and Security Review,* 29(5) (2013), 610.

* My previous publications are in the Irish spelling of my surname (O' Floinn) and are referred to herein as such.

Acknowledgements

I am extremely grateful to the School of Law QMUL for awarding me the Graduate Teaching Assistant PhD scholarship that made this project possible. My supervisors, Ian Walden and Peter Alldridge, have provided constant support, and it has been a pleasure to work with them over the past four years. Ian's perceptive comments and attentiveness to detail have always pushed me to develop my ideas; he has provided unstinting support and encouragement on this project, as well as others en route. Peter warmly welcomed me to the Law Department—prior to even commencing my PhD studies—when I taught with him on the evidence module. He always made himself available, at the shortest of notice, even while packing for holidays!

David Ormerod helped to shape my ideas for this project at a very early stage, prior to moving to the Law Commission. Ever since he has been a friend and a mentor, and has always promoted my work, for which I am grateful.

I would like to thank Giulia Liberatore, Donal Coffey, and Georgia Douglas for commenting on draft chapters, and the participants at conferences organised by the Judicial College, the Office of Surveillance Commissioners, the Institute of Advanced Legal Studies, the European Academy of Law, McKay Law, and the Jill Dando Institute of Security and Crime Science, who commented on various aspects of this work.

My parents, Michael and Mary, I thank you for your encouragement and faith in my abilities, and for always doing everything within your means to support me, and my education. You have both influenced me, and shaped me as a person, in so many ways.

To my brothers, Seán and Eamonn, and my adoptive family, Sergio and Grazia, Francesca and Spence, and Riccardo, thank you for your patience and support. You have all endured this project in so many ways.

Finally, I thank Giulia Liberatore. Your love and support have been unwavering throughout this project. This thesis is dedicated to you.

Abstract

This thesis examines the Council of Europe's Cybercrime Convention and suggests there is a structural imbalance: while improving the procedures for investigating cybercrimes, it has failed to address the prosecutorial complexities and disputes resulting from multijurisdictional cybercrimes, by following the usual trend of 'suppression' conventions. This trend is to expand the procedural mechanisms through which States can acquire evidence in relation to the 'suppressed' offences, while suggesting that State Parties adopt broad rules in relation to criminal jurisdiction. These procedural powers have provided powerful tools for policing cybercrime, and the Convention has been innovative by developing mechanisms for facilitating networking interactions between law enforcement, and on most interpretations, even providing for directly contacting foreign service providers for data. The traditional limitations of enforcement jurisdiction are gradually being transformed, but the resulting difficulties for jurisdictional concurrency are not appreciated. Given the malleability of the concept of 'territoriality', and the flexibility afforded in international law in its interpretation, seizures of jurisdiction over many cybercrimes have sometimes been on the most tenuous of grounds. This results in a problem of concurrent jurisdiction on a scale previously unseen in the context of other transnational offences. It is often assumed that once substantive criminal harmonisation occurs, jurisdictional conflict between States dissipates, but I highlight three areas where concurrency is beginning to generate difficulties: investigatory and prosecutorial negotiations, cybercrime extraditions, and the law relating to *ne bis in idem*. I argue that these problems are only going to be exacerbated given the inroads that are being made in investigative powers and enforcement jurisdiction, coupled with the global reach of cybercrime which brings more and more States into play. I provide both the theoretical and practical case for more refined approaches towards the concept of territoriality, and consider some of the potential mechanisms for dealing with these uneasy bedfellows in the Cybercrime Convention.

Table of Contents

Chapter 1: Introduction 13

1.1 Introduction 13

1.2 Treaties and Transgovernmental Networks: A Powerful Combination 16

1.3 A Structural Imbalance 20

1.4 Methodology 24

1.4.1. Interviews 27

1.4.2. Observations at the COE 31

1.5 Chapter Outline 31

1.6 Looking forward 34

Chapter 2: Jurisdiction in International Law 36

2.1 Introduction 36

2.2 The Territorial Limits of Enforcement Jurisdiction 38

2.3 The Jurisdiction to Prescribe: The Vagaries of Public International Law 40

2.4 Territoriality and Trans-jurisdictional Offences 44

2.5 Extraterritorial Jurisdiction 49

2.5.1. Nationality Jurisdiction 49

2.5.2. Passive Personality 51

2.5.3. The Protective Principle 52

2.5.4. Universal Jurisdiction 52

2.6 Resolving Concurrency? 54

2.6.1. The Principle of Legality 55

2.6.2. Jurisdictional Reasonableness and Ryngaert's Rule of Reason 56

2.7 Conclusion 58

Chapter 3: The Suppression Process 61

3.1 Introduction 61

3.2 Transnational Criminal Law 62

3.2.1. Regularisation of Relationships in the EU 64

3.3 The Formation of Suppression Conventions 67

3.3.1. Critiques of Guzman 69

3.3.2. Rational Choice and Suppression Conventions 70

3.4 The Pattern of Suppression Conventions 74
3.4.1. Jurisdiction 76
3.4.2. Mutual Legal Assistance 80
3.4.3. Extradition 81
3.5 Harmonisation through the Cybercrime Convention 83
3.6 Conclusion 89

Chapter 4: Cybercrime Investigations 91
4.1 Introduction 91
4.2 Extending the Scope of Domestic Procedural Powers 93
4.2.1. Domestic Production Orders 93
4.2.2. The Foreign Service Provider 98
4.2.3. Search and Seizure 111
4.3 The Proposed Protocol 120
4.4 The Role of TGNs 123
4.5 Conclusion 128

Chapter 5: The Ambit of Cybercrime 132
5.1 Introduction 132
5.2 Content Offences 133
5.2.1. Content Offences 1: Hate Speech 133
5.2.2. Content Offences 2: Child Sexual Abuse Images 138
5.2.3. Content Offences 3: Copyright Offences 143
5.3 Computer-Related Offences 149
5.3.1. Fraud Offences in E&W 150
5.4 Computer-Integrity Offences 153
5.4.1. Computer Access Offences in E&W 153
5.5 Conclusion 156

Chapter 6: Addressing Jurisdictional Conflicts: Investigatory and Prosecutorial Negotiations 160
6.1 Introduction 160
6.2 Resolving Conflicts in International Law 162
6.3 Resolving Conflicts of Jurisdiction in EU Law 166
6.4 Negotiating Concurrency 171
6.5 Conclusion 177

Chapter 7: Cybercrime Extraditions 179

7.1 Introduction 179
7.2 Gary McKinnon: A Representative Cybercrime Extradition Case? 181
7.3 Searching for Balance: Flexibility and Obligation in Extradition Law 186
7.4 Dealing with Jurisdictional Concurrency in UK Extradition Law .. 194
7.5 Cybercrime Extraditions 199
7.5.1. US to UK Extradition Requests 200
7.5.2. US Extradition Requests Beyond the UK 202
7.5.3. Finger Pointing and Contributory Causes 208
7.6 Forum Bars 213
7.7 Conclusion 218

Chapter 8: *Ne Bis in Idem* 222
8.1 Introduction 222
8.2 *Ne Bis in Idem* in the EU 225
8.2.1. CISA and Article 54 226
8.2.2. The FR Charter and Article 50 228
8.2.3. The Significance of Protection in the EU 230
8.3 Colangelo and Dual Sovereignty 233
8.3.1. Recognising the Difficulties 235
8.4 The *Idem* Challenge 236
8.4.1. The CJEU's Approach to Idem 237
8.4.2. The Dangers of Convergence Between the ECtHRs and the CJEU .. 240
8.4.3. Rule Against Duplicity v Ne Bis in Idem 244
8.4.4. Idem in the Cybercrime Context 247
8.5 Conclusion 249

Chapter 9: Conclusion 251
9.1 Introduction 251
9.2 Addressing Investigative Challenges: Extraterritorial Data and the Role of Networks 255
9.2.1. Supplementing Networks 259
9.2.2. Subsuming Networks 260
9.2.3. A Double-edged Sword 261
9.3 Addressing Jurisdictional Concurrency 262
9.3.1. More Choices 263
9.3.2. Development of Cybercrime-specific Guidelines for TGNs 265

9.3.3. A Forum Bar in Suppression Conventions 267
9.3.4. Ne Bis in Idem 269
9.4 Conclusion 271
Bibliography 274

Table of Abbreviations

A4P7	Article 4 of Protocol 7 to the Convention for the Protection of Human Rights and Fundamental Freedoms
ASIL	American Society of International Law
CDPA	Copyright Designs and Patents Act 1988
CJA 2003	Criminal Justice Act 2003
CJEU	Court of Justice of the European Union
CJX	Criminal Justice Extranet
CISA	Convention Implementing the Schengen Agreement
CMA 1990	Computer Misuse Act 1990
COE	Council of Europe
CPS	Crown Prosecution Service
DRIP	Data Retention and Investigatory Powers Act 2014
E1, E2, E3, E4	Europol EC3 Interviewees 1, 2, 3, 4.
EA1989	Extradition Act 1989
EA 2003	Extradition Act 2003
E&W	England and Wales
EC	European Community
EC3	European Cybercrime Centre
ECHR	European Convention on Human Rights
ECtHRs	European Court of Human Rights

EDRi	European Digital Rights
EJ	Eurojust Interviewee
FA 2006	Fraud Act 2006
FR Charter	Charter of Fundamental Rights of the European Union.
GNSO	Generic Names Supporting Organization
ICANN	The Internet Corporation for Assigned Names and Numbers.
ILC	International Law Commission
IP	Intellectual Property
J-CAT	Joint Cybercrime Action Taskforce
LEA	Law Enforcement Agency
MLA	Mutual Legal Assistance
MLAT	Mutual Legal Assistance Treaty
OECD	Organisation for Economic Cooperation and Development
OPA 1959	Obscene Publications Act 1959
PACE 1984	Police and Criminal Evidence Act 1984
PCA 1978	Protection of Children Act 1978
PCeU	Police Central E-Crime Unit
PC-YC	Committee of Experts on Crime in Cyber-space
POA 1986	Public Order Act 1986
POA 1936	Public Order Act 1936
RIPA	Regulation of Investigatory Powers Act 2000
S1, S2, S3	SOCA Interviewees 1, 2, 3.

SQ1-4	Sub-questions 1-4
SCA	Stored Communications Act
SUA Convention	Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation
T-CY	Cybercrime Convention Committee
TCL	Transnational Criminal Law
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
TGN	Transgovernmental Network
TOR	The Onion Router
UK	The United Kingdom
UNCAC	United Nations Convention Against Corruption
UNTOC	United Nations Convention Against Transnational Organized Crime
US	The United States of America

Chapter 1: Introduction

1.1 Introduction

Cybercrime[1] is far from the first category of criminality to transcend borders, and to create difficulties for both its investigation and prosecution. But it is unique in the ease with which it can do so. Malicious software (**malware**) can be spread to millions of computers with ease through emails or social networking sites.[2] Child sexual abuse images can be made available to every country in the world with Internet connectivity at the click of a button. Compromised bank account or Paypal details can be purchased for pennies on the pound. The criminal laws of the world can be engaged almost simultaneously by any of these operations, and criminal investigations into these events can be labyrinthine in nature. Such criminals can utilise anonymising software, such as TOR,[3] and diversify their operations across territories, by operating in loose, adaptable, and resilient networks of cybercriminals.[4] Even where individuals are identifiable, evidence in relation to a particular activity could be scattered across numerous territories, or volatile in nature, depending on the retention practices of service providers. These difficulties are compounded where the suspects are physically located in jurisdictions with weak or non-existent cybercrime laws. The Internet has, therefore, transformed criminal behaviour,[5] with multi-victim and multi-State effects routine, on a scale previously unseen, and compounded by technological sophistication in execution and evasion. It is trite to say that this relatively recent criminal phenomenon is difficult for States to suppress; Williams refers to such transnational criminals as "sovereignty-free rather than

[1] The term 'cybercrime' has been subjected to frequent condemnation in the literature due to definitional uncertainties. Wall (2007(b)), 10, for example, describes it as 'meaningless' in and of itself, because of the tendency to use it without a scientific or legal signification. See also Ram (2014), 379. Nevertheless, I will utilise the term 'cybercrime' for the same reasons as Clough (2010), 9: it is frequently referred to in the literature, it is used in common parlance, it emphasises the networked nature of most modern forms of computing, and it is the term adopted in the Council of Europe Convention on Cybercrime (CETS no. 185, Budapest, 2001). In chapter five, I will be adopting the categorisation of cybercrimes found in the Convention.
[2] For an explanation of the use of malware in perpetrating frauds, see MacEwan (2013).
[3] https://www.torproject.org/ (Accessed 20/12/2014).
[4] See e.g. Holt (2013) and Sansom (2009).
[5] See Wall (2007)(b).

sovereignty-bound"[6], while the investigative authorities of States remain bound by traditional norms of sovereignty and international law.[7] National criminal justice systems have never faced a form of criminality where the perpetrators, evidence, and victims, are so globally dispersed, and where such technical expertise is demanded from investigators.[8]

Such jurisdictional challenges generated a substantial body of literature in the 1990s, which either prophesised the end of the Nation State, or contended this traditional construct would have little to do in countering cybercrime. Early cyberlibertarians[9] such as Barlow[10] and Johnson and Post[11] are an extreme illustration, as they argued that 'cyberspace' was a distinct area where territorial governments were unwelcome, predicting that decentralised and self-regulatory efforts of 'netizens' would, and should, govern in this arena. This argument was based, *inter alia*, on the assumption that the networked environment destroyed the ability of States to control online behaviour and generated legitimacy concerns, as some States would attempt to enforce their laws on global phenomena. Cyberpaternalists like Goldsmith, however, observed numerous fallacies in this train of thought, most notably the assumption that cyberspace is a 'distinct area.'[12] This generation of thinkers pointed to the potential for governments to assert control through controlling "code",[13] and dispelled the cyberlibertarian's normative argument against any governmental regulation.

However, the concerns regarding a loss of State control, which sparked this debate, endure. Pinelli speaks of the "circumvention of state borders due to technological developments" and "phenomena such as the return of pirates … in the virtual world […which] seem to bring the world back to the pre-

[6] Williams (1999), 45.
[7] Giraldo and Trinkunas (2009), 440.
[8] Even relatively routine and local 'physical' criminal offences may be complicated, requiring evidence from foreign internet service providers and, thus, use of international legal instruments and inter-State cooperation.
[9] I adopt Murray's labelling of the different phases of thought in this debate: Murray (2013), 56-60.
[10] Barlow (1996).
[11] Johnson and Post (1996).
[12] See e.g. and Goldsmith (1998(a)) Goldsmith (1998(b)).
[13] Reidenberg (1997) and, most notably, Lessig (1999).

Westphalian epoch."[14] Kohl claims "foreign [cybercrime] activity is, in all but exceptional circumstances (e.g. the foreign perpetrator enters the country), … outside [of States'] enforcement jurisdiction even if, as is usually the case, States have in principle a right to regulate it."[15] Guadamuz states "it seems like cybercriminals are usually operating practically unopposed."[16] Indeed, even Susan Brenner, one of the most prominent scholars of cybercrime, claims in her book *Cyberthreats and the Decline of the Nation-State* [17] that "cybercriminals usually get away with their crimes",[18] pointing to extraditions being of "little, if any, use in this context",[19] the problem of 'cybercrime havens',[20] and the ease with which cybercriminals can circumnavigate law enforcement efforts at apprehensions by using masking techniques to hide identifying information.[21] Therefore, Post's challenge to the cyberpaternalists that "[a] world in which, on occasion, bullets are fired from one jurisdiction into another is not 'functionally identical' to a world in which all jurisdictions are constantly subjected to shrapnel from a thousand different jurisdictions",[22] is valid.

Indeed, this shrapnel raises two somewhat antithetical worries. On the one hand, the aforementioned complexity and transnational nature of cybercriminals' activities raises the distinct prospect of under-enforcement, and of States being unable to maintain internal order and security. This can be referred to as the problem of enforcement jurisdiction. On the other hand, the ease with which activities in the networked environment can trigger the criminal laws of multiple countries simultaneously would appear to make conflicts of jurisdiction an inevitability, as States can seek to prosecute offences on the basis of tenuous jurisdictional connections or in circumstances which other States would find disagreeable. This is referred to in this thesis as the problem of jurisdictional concurrency. My thesis investigates how States

[14] Pinelli (2010), 501
[15] Kohl (2014).
[16] Guadamuz (2011), 181.
[17] Brenner (2014).
[18] Ibid, 49.
[19] Ibid, 44.
[20] Ibid, 50-57.
[21] Ibid, 57-60.
[22] Post (2002), 1371.

have responded to these antithetical jurisdictional challenges, focusing, in particular, on how they are addressed in the primary international instrument in the field, [23] the Council of Europe's Cybercrime Convention (**the Convention**).[24] The following sections serve to introduce some of the key and innovative ways through which this instrument has developed — and is developing — in order to deal with these jurisdictional challenges, as well as the areas which have been neglected. I then introduce my methodology for investigating these issues within the thesis, and end with a brief outline of my chapter structure.

1.2 Treaties and Transgovernmental Networks: A Powerful Combination

One of the first issues examined in this thesis are the legal powers that have been afforded to Law Enforcement Agencies (**LEAs**) to tackle cybercrime. I seek to inject a dose of realism into the claims that States are powerless to tackle cybercrime by analysing the mechanics of the Cybercrime Convention.

The Convention is a traditional tool of international law and many doubt its utility for addressing this novel form of criminality.[25] One of the main critiques is that it fails operationally, [26] in that the provisions for transnational cooperation and evidence sharing are too slow and bureaucratic in practice—a particular problem given the volatility of data in the networked environment. However, the Convention has been innovative in many respects, particularly in how it has sought to embrace the benefits of a distinctive form of international cooperation: networked interaction by law enforcement. One form of this is described in the literature as 'transgovernmentalism', which has its roots in the pioneering work of Keohane and Nye[27] in the 1970s. This highlighted a distinctive approach to international cooperation that did not involve the

[23] There have been other harmonisation initiatives, such as the Arab Convention on Combatting Information Technology Offences (League of Arab States, 2010), however, the Cybercrime Convention remains the most significant and widely ratified international agreement.
[24] *Supra* note 1. The United Kingdom ratified the Convention on the 25th of May 2011, and it came into force on the 1st of September 2011.
[25] Goldsmith and Wu (2006), 167 and Goldsmith (2011).
[26] Rozensweig (2012), 420.
[27] Keohane and Nye (1974).

traditional international system of treaty cooperation,[28] but rather a decentralised network of transgovernmental networks (**TGNs**), where participants meet with their counterparts in foreign States in order to exchange information, collaborate, and coordinate action. The State was unbundled by transgovernmental theorists, and rather than disappearing, it was seen to be "disaggregating."[29]

There is no consistent definition of transgovernmentalism in the literature due to the variety and disparate nature of such structures,[30] but Keohane and Nye's broad definition of transgovernmental relations still holds value: "sets of direct interactions among sub-units of different governments that are not controlled by the policies of the cabinets or chief executives of those governments."[31] which are distinguished from traditional inter-State interaction involving heads of state or foreign offices, and "transnational interactions" between private non-state actors.[32] Once these networks are identified, the State is recast "as a supple actor able to capitalize on, rather than be circumvented by, the information age"[33] and many transgovernmentalists claim it will be the "blueprint",[34] and primary vehicle, for international cooperation in the 21st century. As Slaughter notes, "networked threats require a networked response."[35]

---

[28] In their generic senses, the terms 'convention' and 'treaty' are synonymous, and I will use them interchangeably. See the introductory note to the UN Treaty Collection, available at: https://treaties.un.org/pages/Overview.aspx?path=overview/definition/page1_en.xml#treaties (Accessed 20/12/2014).

[29] Slaughter (2004), 12.

[30] Indeed, it has been described as an "arid" exercise to attempt to do so: Newman and Zaring (2013), 253. TGNs are found across all factions of governmental activities and can range from bilateral police networks to more institutionalised organisations, such as the Global Prosecutors E-Crime Network, or the Financial Action Task Force. See Eilstrup-Sangiovanni (2009), 198.

[31] Keohane and Nye (1974), 43.

[32] In their earlier work, Keohane and Nye (1974), 41, footnote 5, defined 'transnational interactions' as occurring where one actor was non-governmental. While this term was later abandoned for adding undue complexity to their general argument, developments in the area of cybercrime investigations make clear that this form of interaction not only requires labelling, but also equal attention to that received by TGNs in the literature. For the purposes of this thesis, I will therefore refer to 'transnational interactions' as that occurring between law enforcement agencies and foreign service providers, which I explore in chapter four.

[33] Raustiala (2002), 22.

[34] Slaughter (2004), 197.

[35] Ibid, 2.

However, the literature on TGNs has largely neglected the interaction between transgovernmentalism and traditional treaty cooperation.[36] Some attempted definitions of TGNs deny that they can be created by treaty.[37] Others recognise that "some treaties provide for network-like relationships, making it difficult to cleanly identify networks as simple alternatives to treaties"[38] but it is generally considered "unusual"[39] for a TGN to be fostered by treaty. Analysis of the Convention, however, tells a different story: it shows how the drafters of the Convention were keen to tap into the benefits of TGNs, and attempted to build such networking interaction into the Convention's architecture, as will be demonstrated in chapter four.

I contend that Raustiala was, therefore, correct to counter claims from some transgovernmentalists who argue "the golden age of the treaty is coming to a close."[40] In the face of seemingly intractable global problems, networks can fill gaps and thus improve the overall effectiveness of treaties,[41] as they are currently doing to deal with the enforcement gap created by the slow and bureaucratic nature of traditional mutual legal assistance (**MLA**).[42] They may also smooth the negotiation of treaties by allowing States to build on pre-existing relationships.[43] Raustiala thus argued that TGNs were more likely to "supplement, rather than supplant, the traditional tools of international law."[44] But I see another reason why networks may not prove to be the death knell of the traditional treaty, at least in the context of cybercrime cooperation; it is because these relationships are likely to be further *subsumed* within the traditional structures.

---

[36] Although the provisions to which I will refer speak of 'Parties', portraying States as unitary actors, as is the norm in such conventions, the drafters no doubt appreciated that these interactions would occur between sub-state actors. As Slaughter (2004), 12 notes, "[i]nternational lawyers … have always known that the entities they describe and analyse as "states" interacting with one another are in fact much more complex entities."
[37] Eilstrup-Sangiovanni (2009), 200.
[38] Newman and Zaring (2013), 252. Alvarez (2011), 212 has also noted how "much of [network] activity arises under the shadow of an intricate web of obligation arising from obligations assumed under treaties."
[39] Raustiala (2002), 12 identified the creation of a TGN in the Convention for the Suppression of the Illicit Traffic in Dangerous Drugs (UNTC no. 4648, Geneva, 1936).
[40] Raustiala (2002), 25.
[41] Ibid, 6.
[42] See discussion in 3.4.2 below.
[43] Ibid, 86.
[44] Ibid, 6.

When the work of these various networking actors (whether fostered by the Convention or not) is understood alongside the traditional procedural powers found in the Convention (such as powers to order extradition) I will show that States are not as powerless as they are sometimes said to be in cybercrime investigations, or at the very least, that such claims lack analytical balance. Indeed traditional requirements found in transnational crime conventions, such as the obligation to ensure domestic powers are available to order confiscation or seizure,[45] take on an entirely new significance in this context; the Convention is being interpreted, for example, to facilitate gaining access to data from globally operating service providers regardless of where the data is, or even where the service provider is established when served with the order.[46] As a result, some LEAs have never found it so easy to conduct an entire criminal investigation involving foreign suspects and foreign evidence without even leaving their offices. These procedural powers have enhanced policing capabilities against cybercrime considerably. However, the widespread belief that "criminals are ahead of the game"[47] is resulting in substantial efforts being made to further expand the policing toolkit. A new protocol to the Convention has been discussed in the Council of Europe (**COE)** which would grant further unilateral enforcement powers allowing, for example, police to hack computer systems in foreign countries, and further embedding the transnational interaction between LEAs and service providers. These developments are transforming concepts of territoriality and the traditional territorial limits of enforcement powers.

Therefore, my analysis of these various investigative powers and the synergy that exists with the networking operations fostered by the Convention will provide ample grounds for agreeing with Wall's statement that police also have

[45] See e.g. Article 12 of the UN Convention against Transnational Organized Crime (UNTS no. 39574, New York, 2000).
[46] See chapter four.
[47] Wall (2007(a)), 190, on the other hand, calls this a "police-originated myth." However, there have been few such correctives to these 'loss of control' discourses in the cybercrime context. More generally, Andreas and Nadelmann (2006), 246 have argued that "from a broad historical perspective, state capacities to detect, deter, and detain transnational law evaders have, if anything, grown substantially. The number of safe havens for criminals across the globe has dramatically shrunk over time as the law enforcement reach of the state has expanded." I will demonstrate how such claims are equally applicable to cybercrime investigations and prosecutions.

"powerful new tools for policing the Internet."[48] For some countries at least, it will be shown that the problem of enforcement jurisdiction is often not insurmountable.

1.3 A Structural Imbalance

The above has introduced some of the ways that States are dealing with the enforcement challenges generated by cybercrime. The other antithetical concern, however—that of jurisdictional concurrency—has received far less attention from States and those behind the Convention. When multiple countries can claim jurisdiction over the same set of actions, problems arise for both the State and for individuals. At the State level, conflicts can arise over whether an act should be prosecuted, or over which State should do so, even if there is agreement on the former. For individuals, there is the risk of extradition to—and prosecution and incarceration in—a distant country, or of multiple prosecutions for the same acts in a multitude of countries.

Some assume that such jurisdictional concurrency is unproblematic in practice, particularly where the various substantive laws concerned have been harmonised,[49] as each State can enforce its laws over local wrongdoers, thus indirectly assisting other States affected by the activities.[50] I contend that this assumption requires re-evaluation. While the harmonisation of offences—a key component of the Convention—can reduce instances of disagreement as to whether an offence should be prosecuted, the Convention does little to assist determinations as to which State should assume the helm in prosecution. In fact, I argue that the Convention, and current efforts to improve it, are almost exclusively oriented towards addressing the enforcement challenges, largely neglecting the issue of jurisdictional concurrency. It follows the usual trend of conventions dealing with transnational crime, which expand procedural and enforcement powers, while seeking to maintain the broadest possible number of jurisdictional bases for prosecution, so as to prevent situations of impunity where no State has jurisdiction to prosecute an offence. One may have assumed

[48] Ibid, 196.
[49] See e.g. Kohl (2007), 220.
[50] These views will be discussed further in chapter six.

that the inherent transjurisdictionality of cybercrime would have resulted in some pause for thought as to the suitability of this approach for this new form of criminality, but the Convention does no more than nudge consultations in situations where more than one Party claims jurisdiction over a particular offence.[51] This too is an example of the drafters seeking to rely upon the benefits and flexibility of TGNs in order to address the difficulties which can emerge from jurisdictional concurrency,[52] but showing no interest in the process or perils of this approach.

My analysis of State practice reveals the malleability of the concept of territoriality when applied to cybercrime,[53] and that prosecutions are brought based on tenuous connections such as the accessibility of the content, or the location of servers storing infringing information. Contrary to claims by Brenner and others, it will be seen that tools like extradition *are* used in cybercrime enforcement, and that they have utility both when they are used to prosecute and convict perpetrators, as well as having value for deterrence purposes. Where extraditions do occur, they are frequently high-profile events, with investigating authorities widely advertising their successes. However, they can be on the basis of weak jurisdictional assertions or at least in circumstances where other States have much stronger jurisdictional ties with the offence alleged. Where such cases are ultimately prosecuted can be determined by factors such as which LEA initiated the investigation, the capacity and willingness to pursue the case, and the influence of actors within TGNs if concurrency is negotiated therein. There is nothing in the Convention or in its supporting documents to assist such deliberations. Nor does it deal with situations where an offender is prosecuted by numerous countries (even consecutively) for the same acts, even though the Convention's drafting Committee was asked to examine the principle of *ne bis in idem*.[54] The current

[51] Article 22(5).
[52] We will also see that the author of one of the most systematic expositions of the concept of jurisdiction in international law, Cedric Ryngaert, has also relied on the potential of networks to resolve cases of jurisdictional concurrency. I critique his conceptual framework in chapter two.
[53] See in particular chapters five and seven.
[54] Explanatory Report, Cybercrime Convention, para. 11. The principle of *ne bis in idem* is the subject of chapter eight and will be explained and explored therein, but broadly speaking, it prevents re-prosecutions for the same acts or offence.

paradigm not only creates a platform for significant potential unfairness for individuals,[55] but it also raises the prospect of further disputes between States. These concerns are particularly warranted when understood in the context of the inroads that are being made to expand the investigative toolkit, as discussed in the previous section.

This thesis argues that there is a structural imbalance in the Convention, and that the breadth of jurisdictional bases—and in particular the breadth of territorial jurisdiction—for prosecuting cybercrimes generates a problem of concurrent jurisdiction on a scale previously unseen, requiring greater attention in the Convention, or any instrument which may supersede it. Assumptions which have driven previous transnational crime conventions, such as the need to maintain jurisdictional breadth in order to avoid safe havens and impunity,[56] and that conflicts stemming from jurisdictional concurrency dissipate where harmonisation occurs,[57] are in need of re-evaluation. In the realm of cybercrime, as will be seen, the architecture of the Internet has particularly strengthened the ability of many States both to conduct investigations, and to claim territorial jurisdiction over offences. The latter is a particularly insidious development. The ease with which States can characterise cybercrimes as territorial offences, despite the offender being based abroad, makes it more difficult to perceive unreasonable assertions of jurisdiction, as the claim to territoriality brings an air of legitimacy to the action. Indeed, it must be questioned whether the very notion of territorial jurisdiction can continue to provide a sufficient basis for determining the place of prosecution, given the way it is currently being interpreted.

---

[55] The lack of harmonisation of procedural safeguards in criminal trials, for example, could see an individual prosecuted in a completely foreign criminal justice system, in a language they don't understand, and subject to criminal penalties that could be many times greater than that which they would receive in their State of nationality.

[56] This assumption, which is discussed in more detail in chapter six, is often related to the enforcement challenges in cybercrime investigations and prosecutions. Kaspersen (2009), 25 notes, for example, that "formal restrictions (mutual cooperation) […] may restrict the number of actual concurring jurisdiction claims." As we will see in chapter four, however, the difficulties associated with formal inter-State cooperation are often not as pronounced as they are said to be, given the variety of alternative mechanisms for securing evidence abroad.

[57] Hayashi (2007), 66 claims, for example, that "[w]hen states reach a consensus on preventing and prosecuting certain crimes and establish a treaty for that purpose, tensions among competing jurisdictions are no longer the main issue."

I am, therefore, primarily concerned with the structure of the Convention and the problem of concurrent jurisdiction and this work ambitiously attempts to analyse the Convention holistically, from a jurisdictional perspective, looking at what its provisions can mean in practice for State Parties. This sometimes demands consideration of wider cooperation frameworks, such as those present between EU Member States, as this is sometimes how States fulfil convention obligations. It is also the reason why the role of TGNs and other transnational interactions between LEAs and service providers are considered, as both the Convention and current attempts at improving it, seek to embrace the benefits of these networking actors in overcoming the challenges posed by the transnational nature of cybercrime investigations.

This emphasis means that cyber attacks by States or so-called 'cyberterrorism',[58] are outside the ambit of this thesis as they are not within the remit of the Convention.[59] I do not consider the work of the intelligence agencies, for access reasons,[60] nor do I provide an account of the various networking actors involved in Internet governance. I neither directly analyse the various discussions that have been occurring within the UN for a new cybercrime treaty,[61] though my examination of the Convention will highlight the challenges that would be faced in any attempt at developing a new international instrument for dealing with this multijurisdictional form of criminality. One further qualification that must be made from the outset is that while many of the developing trends[62] concern the United States (**US**), I do not want this thesis to be read only as a critique of US cybercrime policing

[58] The applicable laws for these activities are considered by Schmitt (2013), Roscini (2014), and Shackelford (2014).
[59] When such activities constitute criminal offences committed by means of computer systems, however, the procedural powers in the Convention are applicable, and these provisions will be analysed. See Article 14(2)(b) of the Convention.
[60] The Snowden revelations have, however, demonstrated the extraordinary powers of the intelligence agencies of the US and the UK, which support my general argument that States have powerful tools at their disposal for policing cybercrime. A further reason for not considering programs like Prism is because they seem to be beyond what is envisaged under the Convention. The Explanatory Report to the Convention (see paras. 182, 219, and 230) states that the provisions relating to production orders, collection of traffic data, and interception, would not authorise the indiscriminate acquisition of such information, which is exactly what these surveillance programs do.
[61] See, for example, the discussions for a new cybercrime treaty during the Twelfth United Nations Congress on Crime Prevention and Criminal Justice (Brazil, 12-19 April 2010). See < http://www.un.org/en/conf/crimecongress2010/ (Accessed 20/12/2014).
[62] See e.g. chapter seven on cybercrime extraditions.

practices. The US is, undoubtedly, the "global hegemon"[63] in the realm of policing power. It has strongly influenced both the normative content and the structure of many 'suppression' conventions,[64] including the Cybercrime Convention, and is at the forefront of enforcement. It is the country that has most demonstrably availed itself of these powers, and is known for its exorbitant exercises of jurisdiction. But even countries like the United Kingdom (**UK**), which has been traditionally conservative on territorial jurisdiction, have interpreted territoriality broadly in the context of domestic cybercrime law.[65] And as the capacities of countries to fight cybercrime increase, I argue the current structure of the Convention lays the groundwork for jurisdictional concurrency to be a much more prevalent and intractable problem between multiple countries, well beyond the US.

1.4 Methodology

My overarching research question was how does the Convention deal with the aforementioned antithetical jurisdictional concerns, and whether its current structure remained coherent for dealing with this inherently multijurisdictional form of criminality. This generated a number of sub-questions:

- How are the jurisdictional challenges inherent in the investigation and prosecution of cybercrime addressed in the Convention, and why has it assumed the form it has? (SQ 1).
- What can the provisions of the Convention mean in practice, and how are jurisdictional concepts (in particular concepts of territorial jurisdiction) developing in State Parties to the Convention? (SQ2).
- What risks and potential problems inhere in the current structure of the Convention and its likely future development? (SQ 3).
- Are there ways the Convention could be improved structurally in order to better deal with the jurisdictional challenges entailed in cybercrime investigations and prosecutions? (SQ4).

This is, therefore, an ambitious study of the Convention at both a macro and micro legal level. It is primarily a doctrinal study,[66] with the Convention being

[63] Andreas and Nadelmann (2006), 243.
[64] See chapter three for an explanation of these instruments, which are international agreements by States that are aimed at suppressing transnational crimes.
[65] This is discussed in chapter five.
[66] As Peczenik (1981), 17 notes, "[b]riefly speaking, doctrinal study of law consists in the interpretation and systematization of (valid) legal norms."

my point of departure, and an analysis of primary sources, namely case-law and legislation, and secondary sources, the starting point for my research questions. SQ1 is addressed almost exclusively from these sources. I analyse the convention through the literature on transnational criminal law, and the theory behind treaty formation (chapter three). I then place the convention in context by examining all transnational crime conventions in order to identify evolutionary patterns across these documents. All publicly available documents relating to the drafting of the Convention were also consulted for this purpose.

SQ2 and SQ3 are the research questions which drive and shape much of the remaining analysis. On the issue of investigative jurisdiction and the concept of territoriality in the realm of procedural powers, I begin with the provisions of the Convention, and then utilised illustrative cases and legislative developments from various State Parties, to demonstrate the scope of these powers. I then turn to the issue of jurisdictional concurrency over cybercrime, with my research hypothesis being that this has been inadequately addressed in the Convention, and will become a more intractable problem as States develop their enforcement capabilities. In order to illustrate the malleability of the concept of territoriality in the realm of cybercrime, I decided upon a jurisdictional case study of all of the cybercrimes found in the Convention, as implemented in the UK. PhD length constraints did not permit for a broader study but the UK was chosen as it was described in the literature as the most jurisdictionally conservative; should territoriality be interpreted broadly here, it would be illustrative of the potential interpretations in other, less jurisdictionally conservative, countries.

This analysis was the platform for exploring the challenges posed by jurisdictional concurrency, as well as assumptions in the literature that it is unproblematic where harmonisation occurs. I selected particular areas of international cybercrime enforcement where jurisdictional concurrency could cause difficulties for States, or individuals. Cybercrime extradition law was chosen as it was an obvious area within the Convention where jurisdictional concurrency could generate difficulties in practice, given the nature of cybercrime. I focus particularly on the extradition practices of the US in the realm of cybercrime enforcement, with a further case study of US-UK

cybercrime extraditions. This focus in my research was for the following reasons: first, the US, a State Party to the Convention, is one of the most active countries in cybercrime extraditions, given its policing capacities in the field. Second, the court documents associated with US cybercrime extraditions are frequently available online, and published on the US Department of Justice website. I searched and analysed all cybercrime extradition cases from this source, in order to identify the jurisdictional bases upon which the extradition cases were built, and to discern any emerging jurisdictional trends. Third, my particular focus on the US/UK cybercrime extradition relationship was based on a research assumption that if difficulties were developing between the UK and US – two policing superpowers and close law enforcement allies – then the stage could be set for such problems to be replicated elsewhere, particularly as cybercrime policing capabilities increase and given the trends in extradition law revealed by my analysis of suppression conventions.

I further problematise jurisdictional concurrency by focusing on the risk of repeated prosecutions for the same cybercrime activities – a possibility where criminal actions engage the laws of multiple countries simultaneously – and investigate how the convention could have addressed this issue. This entailed a study of the international law status of the *ne bis in idem* principle and its application to cybercrime activities.

Aspects of my research questions (in particular, SQ 2) also required that I gather primary data. It was clear from both the text of the Convention (e.g. Article 22(5)), as well as from my literature review, that a key arena for resolving issues pertaining to jurisdictional concurrency was between TGNs of cybercrime prosecutors and investigators. Similarly, my study of the procedural investigative powers found in the Convention also revealed that some of its provisions were being interpreted to permit certain transnational interactions, such as data requests being sent by law enforcement directly to foreign intermediaries. The dynamics of these interactions had not been the subject of previous academic investigation, and it was decided that my analysis of the Convention would, therefore, be supplemented with a qualitative study through a number of interviews with relevant actors. These are explained in the next section.

1.4.1. Interviews

The qualitative aspect of my study primarily investigated two issues: the conduct of negotiations and discussions between TGNs where jurisdictional concurrency was at issue, and the practice of transnational interactions between law enforcement and foreign ISPs. On the former, I set out to study the following: how jurisdictional negotiations and discussions are conducted in practice; the factors taken into account in any forum decisions; the challenges faced by TGNs in this context; and, ultimately, whether claims in the literature that 'jurisdictional reasonableness' could emerge with TGNs, was a feasible prospect, given the complexities of cybercrime investigations and policing capacities. On the latter, I sought to investigate: whether data was being provided between law enforcement and foreign ISPs; how data was being provided and in what circumstances; and understandings of the legal nature of these relationships and the legality of data transfers.

A 'purposive' sample, sometimes called 'judgmental sampling', where participants are deliberately selected due to their unique positions and qualities, was employed for this research. As Berg and Lune explain, "[w]hen developing a purposive sample, researchers use their special knowledge or expertise about some group to select subjects who represent this population."[67]

In relation to jurisdictional concurrency, my literature review revealed that key 'hubs' where these jurisdictional discussions take place were the European Union's Europol and their newly established Cybercrime Centre (**EC3**), and Eurojust,[68] and that non-EU States, including State Parties to the Convention like the US, were also involved in these jurisdictional deliberations. Interviews with individuals involved in the coordination of such meetings were therefore deemed to be a priority. It was also necessary to supplement these interviews with the perspectives of those directly involved in these multi-jurisdictional cybercrime investigations and prosecutions, and to this end, I identified investigators from the cyber division of the then Serious and Organised Crime

[67] Berg and Lune (2012), 52. See also Ritchie et al. (2013), 131.
[68] Both of these organisations will be introduced and discussed in more detail in chapters three and six.

Agency (**SOCA**)[69] as relevant participants. Given that the purpose of these interviews was simply to supplement my doctrinal analysis, and to assist in evaluating some of the assumptions found in the literature on how jurisdictional concurrency should be addressed within these TGNs, it was not deemed necessary to widen the sample.

In relation to the mechanics of the procedural investigative tools found in the Convention, individuals from SOCA were also ideal subjects for interview, given their work in transnational cybercrime investigations. Regarding transnational interactions between LEAs and service providers, it was envisaged that I would "triangulate"[70] my findings from LEA interviews with interviews from between five and ten globally operating service providers in relation to whether—and how—they interact with foreign LEAs. I targeted some of the most prominent service providers in the areas of search, email, social media, online marketplaces, and domain name registrars. These particular services were selected following initial conversations with SOCA officers, who indicated that they had working relationships with some of these entities.

Access to interviewees was secured through a variety of methods. In the very early stages of my research, I developed connections within the cybercrime law enforcement community in the UK, through consultancy work undertaken for Nominet, the .uk domain name registry. This allowed me to identify key senior actors in the SOCA cyber department that had experience in concurrency deliberations with other countries, and/or the conduct of investigations involving data from foreign intermediaries. Three individuals from SOCA were ultimately identified and interviewed. From other previous work experience, I also had contacts within Eurojust, which placed me in a fortunate position whereby I was able to identify and approach a key National Member (a prosecutor) involved in cybercrime coordination meetings. This interviewee further assisted to identify and approach members of EC3 with similar experience at the investigative and coordination level, and ultimately four

[69] This has since merged with the Metropolitan Police Central e-Crime Unit (**PCeU**), to form the National Cyber Crime Unit, within the National Crime Agency.
[70] Berg and Lune (2012), 5 and Silverman (2005), 121.

individuals from EC3 agreed to be interviewed, which included senior members of one of their cybercrime focal points. Access to globally operating service providers was secured through: working through prior contacts, snowballing, and even approaching representatives of service providers directly at conferences requesting interviews.

I conducted interviews with legal representatives of five service providers in the initial stages of the project, however, this aspect of my research became less fruitful as my work progressed. When I began my research, some information existed which suggested that globally operating service providers were providing data to foreign law enforcement,[71] however, it was not a phenomena that was well known outside of those involved in the process. This changed during my research period, as service providers began publishing transparency reports, and openly acknowledging that they had relationships with foreign LEAs.[72] Therefore, one of my key initial queries relating to *whether* such interactions were occurring began to be confirmed without my empirical investigation. After the Snowden revelations, representatives from these service providers also became much less willing to discuss their data sharing practices with researchers. Nevertheless, the five interviews which were conducted with service providers about their relationships with foreign law enforcement, yielded valuable data in relation to the practice and legality of these transnational interactions, and informed my analysis of whether and how the Convention can be said to regulate these relationships.

Ultimately, the following were the number of interviewees included in my study: Eurojust (1), Europol/EC3 (4), SOCA (3), service providers (5). Interviews were generally held in participants' place of work, although in two cases involving service providers, phone interviews were conducted as it was impractical to travel to their offices.[73] All interviewees were provided with a background information sheet in relation to my research, and were given

[71] Some service providers' guides for law enforcement had been leaked. See e.g. Facebook Law Enforcement Guidelines (2009) V0909.2.AA, at 8. Available at: https://info.publicintelligence.net/Facebook2009.pdf (Accessed 20/12/2014). However, the companies often did not confirm the existence of such initiatives, or the authenticity of such documents. See http://blog.legalsolutions.thomsonreuters.com/law-and-techology/facebook-and-police-warrants-can-they-really-do-that/ (Accessed 20/12/2014).
[72] See chapter four, section 4.2.2.
[73] One of the interviewees, for example, is based in Canada.

various assurances, including confidentiality and the choice of remaining anonymous. Permission was also sought to use a digital recorder,[74] and all but one of the participants (a service provider) agreed to this. I transcribed all interviews myself, and they were password protected. Interviews were "semi-standardised",[75] given the exploratory nature of my research, which allowed me to ask a series of regularly structured questions, but also to deviate and digress where appropriate.

The interviews were normally organised around three sections. I began by reiterating the purpose of the study (which had also been made clear in the information sheet) and the potential data usage. The next section involved gathering general information about the work of the interviewee. I then focused on the key issues of the study. In all interviews I had prepared a list of questions that were divided according to my research aims and the areas of relevance identified in the opening paragraph to this section. In my interviews about jurisdictional concurrency, these questions revolved around the following general areas: how forum for prosecution in relation to transnational cybercrimes come to be discussed between law enforcement from different countries; the practicalities of these discussions and any criteria relied upon for determining forum; and any practical problems or challenges which the interviewee has perceived in the conduct of these deliberations. Interviews concerning data provision between service providers and foreign law enforcement were similarly divided into sub-sections (e.g. questions concerning whether data is provided, in what circumstances, the procedures followed and practicalities, legal understandings of powers to request/send data). I followed the same general categories for my interviews with law enforcement and service providers concerning transnational access to data, and this structured approach helped with the triangulation of the data. The flexibility of a semi-structured interview did, however, allow for modification and movement across my questions and for the pursuit of avenues of relevance when they arose.

---

[74] While there is debate amongst research methodologists as to whether such devices benefit or hamper (by inhibiting participation and openness) research, it is now generally accepted that comments should be captured as accurately as possible. See Warren and Karner (2005), 12.
[75] Berg and Lune (2012), 112.

No serious ethical issues were expected in my research, given that all participants were professionals, and I was not seeking information in relation to any on-going investigations. Participation in the research was entirely voluntary with informed consent.[76] I also sought permission to conduct my research from the QMUL research ethics committee, which was granted on the 29th February 2012.

1.4.2. Observations at the COE

Early in my research it was learnt that the COE's Cybercrime Convention Committee (the **T-CY**) had created an "[a]d-hoc sub-group of the T-CY on jurisdiction and transborder access to data" (the **Transborder Group**).[77] They were tasked with developing an instrument (e.g. an amendment to the Convention, a protocol, or recommendation) "to further regulate transborder access to data and data flows, as well as the use of transborder investigative measures on the Internet." I closely followed the work of this group and attended two public hearings where the Transborder Group were presenting and discussing their recommendations.[78] I participated in both hearings—asking questions of members of the TG—and took detailed notes on the various perspectives of attendees.[79] I also wrote an academic commentary on the first meeting.[80]

1.5 Chapter Outline

My second chapter is a literature review of the different jurisdictional concepts which are of pertinence to this thesis. I also consider existing academic proposals for resolving jurisdictional disputes, and argue that these proposals are not equipped to deal with the complexities of cybercrime. This analysis assists to explain why the drafters of the Convention have not chosen to prioritise jurisdictional bases for prosecution, and resigned themselves to

[76] Ibid, chapter three.
[77] TCY 6th Plenary decision (23-24 November 2011).
[78] Notably, a public hearing on transborder access on 3 June 2013, and the Octopus Conference on Cooperation against Cybercrime, 4-6 December 2013.
[79] This included State representatives, NGOs, LEAs, service providers, and various other groups and international organisations.
[80] O'Floinn (2013).

suggesting consultation in the case of conflict. My review of the literature similarly points to the role of TGNs in dealing with jurisdictional concurrency, and this is analysed further in chapter six in light of my interview findings.

SQ1 is addressed in chapter three which investigates the phenomenon of 'suppression' conventions for dealing with transnational crime. It analyses the theory behind the formation and design of such instruments and outlines certain patterns that have developed across them. I then use these theoretical and historical analyses to analyse the Cybercrime Convention and demonstrate how it fits this traditional mould of being an exclusively law enforcement oriented measure, blind to potential consequences for jurisdictional concurrency.

SQ2 – SQ3 are partly addressed in chapter four, and the purpose of this chapter is twofold. First, it introduces some analytical balance into the debates concerning the loss of State control over cybercrime. Second, it demonstrates my claims in chapter three concerning the pattern of suppression conventions: I dissect some of the procedural powers found in the Convention, and show how these can be, and are being, relied upon in practice, in order to extend the arm of domestic law enforcement. The Convention has been innovative in embracing the role of TGNs (through for example, the creation of 24/7 networks of LEAs), and it is also said to permit direct transnational interactions between LEAs and foreign service providers. I also analyse a number of proposals concerning the further extension of transnational access powers, both through expanding unilateral search capabilities, and further entrenching the networking abilities of LEAs.

I then shift the focus from my analysis of territorial jurisdiction in investigative powers, to the issue of substantive criminal jurisdiction, and chapters five to eight focus on SQ2 and SQ3 in this context. Chapter five focuses on SQ2 in particular, and analyses the way territoriality over cybercrime has been interpreted in the UK, a State Party to the Convention that has traditionally been seen to have one of the most restrictive approaches towards criminal jurisdiction. A comprehensive analysis of the criminal laws of England and Wales shows how, in the context of all of the offences found in the

Convention, these laws allow for the most expansive of claims to territorial jurisdiction. The remaining three chapters of the thesis problematise the jurisdictional concurrency which results from this potential breadth of exercise, each focusing on a different phenomenon: jurisdictional determinations between TGNs, cybercrime extraditions, and the *ne bis in idem* principle.

Chapter six first considers the limited ways through which harmonisation initiatives have sought to address jurisdictional concurrency or resolve instances of jurisdictional conflict between States. I then discuss my interview findings, which reveal the reasons behind low levels of conflict between prosecutors and LEAs, but show how such negotiations are increasing in volume in forums like Eurojust, and illuminate the practical difficulties which are arising for law enforcement in cybercrime policing.

My seventh chapter investigates a crucial enforcement tool that is now found in all suppression conventions: the power to extradite offenders. I assess the aforestated claims that extradition is of little use in the context of cybercrime policing, and find it lacking. This chapter demonstrates how States can enforce their cybercrime laws, and illustrates the problems that can emerge as a result of such jurisdictional exercises. I focus particularly on the receipt of cybercrime extradition requests in the UK, but also provide a jurisdictional analysis of a number of cybercrime extradition requests sent by the United States to other countries. I trace the UK's historical treatment of jurisdictional concurrency in extradition cases, in order to explicate the forces which have shaped recent domestic structures, and how these structures facilitated the political and normative difficulties which emerged from various cybercrime extradition requests. The harmonisation process is driving States to expedite extradition procedures, as occurred in the UK, paving the way for the UK experience to be replicated in other Parties to the Convention.

My final chapter considers an area of law which the drafting group behind the Convention were specifically asked to address, but did not: the principle of *ne bis in idem*. I posit that the EU example strengthens the argument that harmonisation of criminal laws and facilitating inter-State cooperation in the movement of evidence and individuals, requires a concurrent strengthening of

this principle operating between States. Current theories that purport to explain the absence of any inter-State version of this principle in international human rights documents, are critiqued and found wanting. Nevertheless, I highlight the difficulties which cybercrime will generate in any application of *ne bis in idem* between States, and consider the perils—most notably the risk to individuals of multiple, consecutive prosecutions—of not dealing with it within the Convention.

I conclude by considering SQ4 in light of my previous findings, and investigate some of the ways that States may be able to attempt to address the jurisdictional tensions that are being created through the expansion of enforcement powers and capabilities, against a crime that—by its nature—implicates the laws of multiple States.

1.6 Looking forward

This thesis is innovative in a number of respects. It is descriptively and empirically innovative by demonstrating how the Convention is operating in practice, with a number of case studies, and by bringing together a range of perspectives from cybercrime prosecutors, investigators, and legal representatives of service providers. It is analytically innovative in its holistic critique of the Convention, and by engaging with the work of a number of commentators: literature on the concept of territorial jurisdiction in international law is critiqued taking into account the specificities of cybercrime, and its investigation and prosecution; rational choice theory is applied in order to understand the structure of the Convention; and I also critique and develop the work of a range of commentators in discrete fields within international law, including transnational criminal law, extradition law, and cybercrime law. Finally, this work is normatively innovative, by challenging jurisdictional interpretations of the concept of territoriality in both investigative and criminal jurisdiction, and by suggesting avenues for addressing jurisdictional over-reaching within the suppression process. Ultimately, my analysis draws attention to the challenges, and opportunities, generated by networked operations and attempts to build them into the structure of the Convention. The work of these actors can have profound

consequences for States and individuals, yet they operate with opacity; this thesis shines a light on their functioning. There are reasons to doubt that "networks will interact with treaties in a manner that promotes stronger, more effective international law."[81] While appreciating the flexibility and other benefits that are the product of networked cooperation, I argue there is a strong need to inject further oversight and more formalised processes, and for rights-based concerns to be addressed more directly. I do not seek to—or pretend to be able to—identify a silver bullet that would outline the perfect synergy for networked interaction, and how (or whether) it should be built into the Convention. However, I will elucidate some of the choices which States have to make to this end, and highlight some of the potential perils of the current trajectory, which seeks to expand unilateral enforcement powers and facilitate the operation of networks under the shadow of the Convention, whilst ignoring the challenges presented by jurisdictional concurrency.

[81] Raustiala (2002), 51.

Chapter 2: Jurisdiction in International Law

> "All crime is local. The jurisdiction over the crime belongs to the country where the crime is committed."[1]

2.1 Introduction

The Treaty of Westphalia 1648 heralded a new system of secular power based on territoriality, such that legal jurisdiction became "congruent with sovereign territorial borders."[2] However, the concept of jurisdiction has rightly been described as "[o]ne of the most difficult words in the legal lexicon to delineate."[3] It derives from the Latin *juris dictio* which means 'administration of justice.'[4] In the context of international law it has been described as "a State's right … to regulate conduct in matters not exclusively of domestic concern."[5] Public international law therefore assumes a regulating role, preventing jurisdictional assertions by States in the absence of a sufficient nexus with the situation. For this reason, it is also tied to the principle of non-intervention and the sovereign equality of States.[6]

Understanding the meaning of 'jurisdiction' is complicated by its divisibility into distinct, yet sometimes overlapping, concepts. It is generally accepted that there is a three-part division between competences to regulate transnational activities: prescriptive jurisdiction, adjudicative jurisdiction, and enforcement jurisdiction. Applied to criminal law, the jurisdiction to prescribe refers to a State's power to establish the content and scope of criminal law in relation to particular situations. As O'Keefe notes, it is the "authority under international law to assert the applicability of its criminal law to given conduct, whether by primary or subordinate legislation, executive decree or, in certain circumstances, judicial ruling."[7] Adjudicative jurisdiction, on the other hand, involves persons or things being subject to the process of a States' courts in

---

[1] *MacLeod* [1891] AC 455, 458, *per* Lord Halsbury.
[2] Raustiala (2005), 2509.
[3] George (1966).
[4] Kohl (2007), 14.
[5] Mann (1964), 9.
[6] Ryngaert (2008), 6 and Crawford (2012), 447.
[7] O'Keefe (2004), 736. See also §401(a) Restatement (Third) of US Foreign Relations Law.

criminal proceedings,[8] while enforcement jurisdiction "refers to a state's authority under international law actually to apply its criminal law, through police and other executive action, and through the courts."[9] In the civil sphere, distinguishing between jurisdiction to prescribe and jurisdiction to adjudicate can be important, as they do not coincide in situations where a court applies foreign law. However, in the criminal sphere, they have been said to be "one and the same."[10] If a State has jurisdiction to prescribe criminal laws to a situation, then its courts will almost invariably have jurisdiction to apply those rules.[11] While there is also some overlap between enforcement jurisdiction and adjudicative jurisdiction,[12] as courts apply and enforce criminal law,[13] enforcement jurisdiction is much more clearly distinguished from prescriptive jurisdiction; it is not concerned with whether a State can prescribe laws with an extraterritorial scope, but with "the lawfulness of the State's own *acts* to give effect to such regulation."[14]

In the introduction to this thesis, I noted two antithetical concerns: the problem of enforcement jurisdiction and the problem of jurisdictional concurrency. Cybercriminals are largely seen to be operating beyond the reach of the State, due to the latter's inability to enforce its laws against perpetrators in foreign locations, and to conduct investigations when evidence in relation to the offence may also be abroad. As I will demonstrate in subsequent chapters, these are often not insurmountable challenges for some States.

In this chapter I provide a review of how these jurisdictional concepts are understood in the literature. I will first outline the concepts and principles that constrain State enforcement action, in order to provide a jurisdictional lens for my investigation of how the Convention – and efforts to amend and supplement it – deals with these traditional territorial restraints. I then turn to the issue of jurisdictional concurrency, and outline the circumstances where

[8] Clark (2014), 92. See also Ryngaert (2008), 10.
[9] O'Keefe (2004), 736.
[10] Akehurst (1972-3), 179. See further, Kohl (2007), 16 and Kreß (2006), 577.
[11] However, awareness of the difference between them is still important since a court may not have jurisdiction to adjudicate, for example, due to an international immunity, even if the State would ordinarily have prescriptive jurisdiction over the offence.
[12] Mann (1973), 128.
[13] Kohl (2007), 18. Emphasis added.
[14] Mann (1984), 154. Emphasis added.

States can, under international law, prescribe their criminal laws over activities that are not exclusively domestic in nature. We will see that international law has long recognised seizures of criminal jurisdiction on broad grounds. Therefore, jurisdictional concurrency is not a new phenomenon, and there are various accounts within the literature as to how it should be addressed. However, I will argue that existing theories are ill-equipped to deal with the complexities of cybercrime. This sets the context for my critique of the substantive criminal jurisdictional provisions in the Convention, and my problematisation of jurisdictional concurrency in chapters six to eight.

2.2 The Territorial Limits of Enforcement Jurisdiction

Enforcement jurisdiction is said to be strictly territorial. It was noted in the now infamous *Lotus* case to be "the first and foremost restriction imposed by international law"[15] stipulating that a State "may not exercise its power in any form in the territory of another State",[16] failing the existence of a permissive rule to the contrary. This is a reflection of territorial sovereignty derived from principles of non-intervention and the sovereign equality of States.[17] A State cannot exercise enforcement jurisdiction outside its own territory in the absence of legislative authority, and even with this authority, the act may not be internationally lawful.[18] As Mann notes, "[t]here can be no question of the two jurisdictions [prescriptive and enforcement] necessarily coinciding."[19] Without consent for the enforcement action, "the rights and privileges of the territorial sovereign prevail."[20] Akehurst expands upon the circumstances which generate such jurisdictional problems stating that an "act of one State in the territory of another may usurp the sovereign powers of the latter either because of the nature of the act or because of the purpose for which the act was done."[21] If an act is a governmental function, it will be illegal by its nature.[22] If

[15] *SS Lotus (France v Turkey)* [1927] PCIL Reports, Series A No. 10, [45].
[16] Ibid.
[17] Ryngaert (2008), 6. On the application of the principle of non-intervention see Wood and Jamnejad (2009) and in the cyber context, see Gill (2013).
[18] Mann (1984), 154.
[19] Ibid, 155.
[20] Ibid, 157.
[21] Akehurst (1972-3), 146.
[22] See further Gill (2013), 222.

the purpose of the act is to enforce the investigating State's law, it will similarly be contrary to international law.[23]

It is natural to attempt to transpose these fundamental rules to the online world. Ziolkowski argues that enforcement activities by foreign LEAs "in networks and computers located on [another] State's territory and outside of a cooperation framework or otherwise without a prior consent"[24] would certainly be unlawful. However, such activities are clearly not as clear-cut as the paradigmatic unlawful activities involving foreign acts (e.g. kidnapping a suspect in a foreign territory). The 'real problem' today may no longer be "ascertaining the limits within which a State can act in a foreign State to enforce its laws",[25] but ascertaining when in fact an act is foreign in the first place. As Kasperson notes, authorities "are not always aware and able to establish that a search extends to computer systems and data located in territories of other States."[26] An even more basic illustration of the problems of transposition here is where an investigating officer is communicating with a suspect through social media, but does not necessarily know where the target is located.[27] Akehurst[28] and Mann[29] are both united in the view that inquiries by police abroad for the purposes of enforcing domestic criminal law are illegal, but does this apply where the officer is not physically present in the place where the inquiries are made? Mann's contention that "*investigations* carried out by or on behalf of a State in a foreign country do not appear to have given rise to fresh problems"[30] is certainly dated given the predicaments faced in modern criminal investigations, particularly those of an 'online' nature. The concept of territoriality in the realm of enforcement power is undergoing transformation,[31] with geographical location becoming harder to determine,[32] and law enforcement intensifying their networking with LEAs and service

[23] Akehurst (1972-3), 146-7.
[24] Ziolkowski (2013).
[25] Mann (1984), 157.
[26] Kaspersen (2009), para. 76.
[27] Discussed in O'Floinn and Ormerod (2011), 786-7.
[28] Akehurst (1972-3), 147.
[29] Mann (1984), 223, footnote 82. "It should, however, be clear that enquiries carried out by the police in a foreign country without its consent are illegal."
[30] Ibid, 161.
[31] See chapter four. For a more general critique of the legal construct of territoriality see Sassen (2013) and Raustiala (2005).
[32] Raustiala (2005), 2513.

providers in foreign countries and routinely interacting with computer systems in foreign territories.[33] Cybercrime investigators may well be expected to take advantage of the malleability of territoriality[34] as a legal construct in the realm of enforcement jurisdiction, and are doing so. And as we shall see in chapter four, legislators and judges have been quick to follow suit. Recent legislative action in the UK, for example, has made an overt attempt to elide prescriptive and enforcement jurisdiction—despite Mann's cogent arguments for their separation above—in order to foster the transnational interactions between LEAs and foreign service providers.[35]

It is certainly true that the territorial nature of enforcement jurisdiction continues to be a significant constraint on the activities of cybercrime investigators, but the advent of the Internet has meant that the hitherto sacrosanct territorial nature of enforcement jurisdiction has become shrouded in ambiguity. This brings challenges, but also opportunities for the law enforcement community, as borders become ever more permeable for them as well as for criminals. As will be elaborated upon in subsequent chapters, the Convention, and current efforts to amend and supplement it, are geared towards furthering the circumstances where LEAs can operate transnationally in order to secure data held abroad. It also facilitates gaining custody of foreign cybercriminals, thus allowing enforcement of criminal laws. It is to the jurisdictional scope of these laws that I turn to next.

2.3 The Jurisdiction to Prescribe: The Vagaries of Public International Law

The *Lotus* case sparked a debate concerning prescriptive jurisdiction which is yet to be theoretically settled. While in the realm of enforcement jurisdiction, a strict territorial approach was adopted, limiting extraterritorial actions unless there was a permissive rule allowing for same, this was not found to be

[33] This transnational accessing of foreign computer systems obviously occurs with almost any use of the Internet. See chapter four for discussion both of how the Convention addressed even these basic extraterritorial exercises of enforcement power (e.g. searching publicly available pages on the web), and current attempts to further expand the circumstances where LEAs can access data over the Internet.
[34] Sassen (2013), 24.
[35] See discussion of Data Retention and Investigatory Powers Act 2014 in chapter four, section 4.2.2.1.

appropriate for prescriptive jurisdiction. Here, States were said to be able to "extend the application of their laws and the jurisdiction of their courts to persons, property and acts outside their territory"[36] as international law left them a "a wide measure of discretion which is only limited in certain cases by prohibitive rules."[37] This liberal approach has met with strong opposition in the literature, and is now widely accepted not to represent customary international law.[38] The practice of States, and opinions of scholars and judges,[39] adopts a 'modern approach' that sees international law as prohibiting "States from exercising jurisdiction as they see fit, unless there is a permissive rule to the contrary."[40] On this approach, territorial jurisdiction is seen as the fundamental rule of the international jurisdictional order, with international law also 'permitting' exercises of jurisdiction on 'extraterritorial'[41] grounds in certain exceptional cases.[42]

While dominant, the modern approach is not free from criticism. One argument is that it is out of tune with the realities of sovereign power. D'Aspremont defends the traditional *Lotus* perspective, critiquing the modern approach for its "strong constitutionalist overtones, for it conveys the impression that international law bears some resemblance to a constitution that define[s] the competence of all public actors."[43] He argues that the distribution of jurisdiction theory inherent in the 'modern' approach fails because it needs to rely on second level rules (such as reasonableness and the principle of non-

[36] *Lotus*, *supra* note 15, [46].
[37] Ibid.
[38] As Ryngaert (2008), 27, notes, "customary international law based on actual State practice turns *Lotus* upside down."
[39] It was said in one case to represent "the high water mark of *laissez-faire* in international relations, and an era that has been significantly overtaken by other tendencies." *Arrest Warrant* (*Democratic Republic of Congo v Belgium*) [2002] ICJ Reports 3, separate opinion of Judges Higgins, Kooijmans and Buergenthal, [51].
[40] Ryngaert (2008), 21.
[41] This term is frequently confused in the literature, and is often said to apply in cases where States are actually invoking territorial jurisdiction (e.g. 'effects' jurisdiction, which is explained below). I follow Ryngaert (2008), 7 in his contention that in the realm of prescriptive jurisdiction, extraterritoriality only refers to assertions of jurisdiction "based on the personality, protective, or universality principle of jurisdiction."
[42] Ibid, 28-9.
[43] d'Aspremont (2010), 310. For a defence of sovereign constitutionalism, see Fassbender (2003).

intervention), which are not certain enough to curtail unilateral exercises of jurisdiction.[44]

A further problem—applicable to either account—is that the normative justifications for the right to punish in the doctrine, particularly its extraterritorial dimension, are often undeveloped, undefined, or simply assumed. Cook, for example, contends that exceptions to territorial jurisdiction are simply "based upon ideas of social expediency."[45] One exception to this is Chehtman's work on the philosophical foundations of extraterritorial punishment.[46] Chehtman draws on a Hohfeldian interest theory of rights which requires identification of particular interests in order to confer upon States the power to punish. He proposes a theory of sovereignty,[47] which is underpinned by a claim-right to territorial integrity (required in order to ensure individuals' well-being and physical security), and a right to self-government (which accounts for States' powers to criminalise and punish certain behaviours in order to meet those ends).[48] The latter right also explains why territorial States hold a *prima facie* immunity from other States extraterritorially applying criminal law on its territory.[49] He contends that:

> a state's prima facie power to punish an offender is based on the collective interest of individuals in that state in its criminal laws being in force. This is because having a system of criminal rules in force constitutes a public good that contributes to the well-being of individuals who live under it in a certain way.[50]

Therefore, a State's right to punish is seen primarily as territorial, and extraterritorial States are under a *prima facie* disability from punishing offences which are perpetrated abroad.[51] This is based on the lack of interest of the populations of extraterritorial States in applying their criminal laws to foreign situations, as well as the aforementioned immunity enjoyed by the territorial State, which stems from the right to self-government.[52] Chehtman is controversial in that he rejects some grounds of jurisdiction considered to

[44] d'Aspremont (2010), 314.
[45] Cook (1934), 328.
[46] Chehtman (2010).
[47] Ibid, 24.
[48] Ibid, 25.
[49] Ibid, 28.
[50] Ibid, 31.
[51] Ibid, 58.
[52] Ibid.

represent customary international law. While jurisdiction based on territoriality, the protective principle, and even universality over international crimes, can be accounted for within his rights-based approach to jurisdiction, jurisdiction based on active nationality, or passive personality, are rejected.[53] The underlying reasons for this will be highlighted below, but of most importance, for the purposes of the present thesis, is Chehtman's lack of consideration of the issue of when a crime can be said to be committed within a particular territory. He contends that this "is a complicated enough question the consideration of which merits treatment beyond the object of this enquiry."[54] This is most unfortunate, given that such a large majority of modern crimes (particularly cybercrimes) are transnational offences, and the omission therefore detracts from the practical relevance of his cogent philosophical arguments.

It is beyond the scope of this work to analyse the competing conceptions of sovereignty and international law underpinning the modern and traditional approaches to extraterritorial jurisdiction. While there is a recognised theoretical stalemate,[55] consensus has formed in the doctrine, which adopts the restrictive modern approach, whereby States must justify their jurisdictional assertions based on a permissive rule of international law. These permissive rules have, however, been interpreted widely. As Ryngaert argues, "the indeterminacy of 'connections' and 'interests' has made States' room for action actually very broad, which has led to an internationally sanctioned system of possibly harmful concurrent jurisdiction."[56]

The next section discusses the "least contested of all [linking factors] in international law",[57] namely, territorial jurisdiction. It will be seen that although it is "universally accepted"[58] that States are competent to punish crimes committed within their territory, this fundamental rule has actually

[53] Ibid, 59-69.
[54] Ibid, 57.
[55] Ryngaert (2008), 20.
[56] Ibid, 22.
[57] Pirker (2013), 196.
[58] Harvard Research in International Law, 'Draft Convention on Jurisdiction with Respect to Crime', *American Journal of International Law*, 29 Supplement (1935), 480. (**Harvard Research (1935)**).

generated the most difficulties for States and scholars, given the malleability of territoriality as a legal construct.[59]

2.4 Territoriality and Trans-jurisdictional Offences

It has long been recognised that a State can exercise jurisdiction over acts which constitute domestic crimes and have been committed "in whole or in part"[60] within its territory. In 1935, in an effort to codify international law by the American Society of International Law (**ASIL**), two separate territorial principles were identified within national legislation and jurisprudence. The first was the subjective principle, which provides jurisdiction when a crime was "commenced within the State but completed or consummated abroad."[61] The second was the objective principle, which provides a power to prosecute and punish when a crime was "commenced without the State but consummated within its territory."[62] Although the issue of which of these States, if any, should enjoy priority was a topic debated in the literature at the turn of the last century,[63] by the time ASIL drafted its convention it was realised that "the arguments were so evenly matched"[64] that neither, taken alone, could explain contemporary practice, and there was no reason for prioritising one over the other.[65] Thus, when any "essential constituent element"[66] was committed within a territory, that State could seize jurisdiction over the crime.

As mentioned above, Chehtman did not address this issue, choosing only to consider the 'standard' cases where both conduct and effect occur within a single territory.[67] His analytical claim that there is a necessary link between having a legal system in force and a State's power to punish, and normative claim that having criminal laws in force contributes to individual's sense of dignity and security,[68] would offer no way of determining which State ought to

[59] See *supra* note 31.
[60] Harvard Research (1935), Article 3 of the Draft Convention.
[61] Ibid, 484.
[62] Ibid, 488.
[63] Akehurst (1972-3), 152.
[64] Ibid.
[65] Harvard Research (1935), 494.
[66] Ibid, 495.
[67] Chehtman (2010), 57.
[68] Ibid, 37.

have the *primary* interest in punishing, and therefore which States were under *prima facie* disabilities from doing so. Both the State where the crime was initiated, and the State(s) where the effects were felt, could claim the action puts into question the existence of that State's legal rules prohibiting the crime, thus affecting its population's collective interest in this public good. All would have an interest in punishing the conduct, and it is not clear which would enjoy the *prima facie* immunity from other States applying their laws to the situation.

Today, international law continues to recognise both the subjective and objective principles of territoriality,[69] but they are not free from controversy, most notably because it is domestic law, rather than international law, that defines what the 'constituent elements' of a crime are. A variety of interpretations have emerged, particularly in relation to how the effects of criminal conduct are to be dealt with.[70] Often in the criminal context, the effects of a crime will also form an element of the offence,[71] but some authors separate the effects and essential elements approaches.[72] According to Ryngaert, "international law seems to have satisfied itself with requiring that either the criminal act or its effects have taken place within a State's territory for the State to legitimately exercise territorial jurisdiction."[73]

The criminal law of England and Wales further complicates this picture, as it has developed a unique theory of jurisdiction which is distinct from the 'constituent elements' approach common to many continental-European countries and the US.[74] The ambit of English criminal law has traditionally been strictly territorial. Unlike the legislative techniques of continental countries, where criminal codes often contain the elements of the crime and jurisdiction is dealt with in a separate chapter, the definition of a criminal

[69] Ryngaert (2009), 189.
[70] In one US case it was even said that "international law principles have expanded to permit jurisdiction upon a mere showing of *intent* to produce effects in this country…" *United States v Noriega* 746 F. Supp. 1506 (S.D. Fla 1990), 1513. For critique, see Bassiouni (2014), 378.
[71] In *Lotus*, and in an example provided by ASIL, the consequences or 'effect' of the criminal act were constituent elements (death being the consequence as well as an element of the criminal act of manslaughter and murder respectively). Harvard Research (1935), 502. See further Kohl (2007), 91.
[72] See e.g. Akehurst (1972-3), 154-5.
[73] Ryngaert (2009), 188.
[74] Ibid, 189.

offence in England and Wales normally includes its jurisdictional ambit.[75] As Hirst notes, "misconduct committed outside the realm cannot ordinarily amount to the *actus reus* of an offence under English law."[76] Therefore, determining the *ratione loci* of an offence is not only a jurisdictional issue, but also one of criminal liability. However, the English approach to cross-frontier offences does not fall straightforwardly within either the subjective or objective approaches to criminal jurisdiction. Even if some elements or effects of a crime are committed or felt within England and Wales, the offence may still not be regarded as having been 'committed' within the territory.[77]

The 'terminatory' approach, christened by Glanville Williams,[78] asks where the crime was *completed*, that is, where the last constitutive act takes place.[79] The 'constituent elements' approach, on the other hand, does generally accommodate the subjective and objective principles of territoriality, and is the dominant approach adopted by the States studied by Ryngaert.[80] These States make full use of the flexibility afforded by international law in seizing criminal jurisdiction. This is done when either a constituent element of the offence, or its effects, occur within the jurisdiction, and some States even assume jurisdiction on the basis of effects which do not form constituent elements of the crime.[81]

Both approaches are riddled with practical problems which have been exacerbated with the advent of cybercrime. The 'terminatory' theory has the theoretical benefit of being a more conservative jurisdictional approach, thus limiting the potential for international conflict due to concurrent jurisdiction. However, the restrictive nature of this approach has already come under pressure in practice and has been abandoned by the legislator for trans-border fraud and dishonesty, in favour of a constituent elements approach.[82] Moreover, the 'terminatory' theory has been plagued by inconsistencies in

[75] Ibid, 87.
[76] Hirst (2003), 3.
[77] Ibid, 113. See further Ryngaert (2009), 193.
[78] Williams (1965).
[79] Hirst (2003), 115. See further Goode (1997), 439 and Ryngaert (2009), 192-3.
[80] These include the US, France, Germany, the Netherlands and Belgium. Ryngaert (2009).
[81] Akehurst (1972-3), 153. See further Ryngaert (2009), 198.
[82] For discussion of the jurisdictional rules pertaining to fraud offences in the UK, see chapter five, section 5.3.1.

application, with case-law showing a variety of ways to manipulate its restrictive effect. An early example was the theory of constructive presence (where presence is assumed to follow the criminal acts of the accused),[83] with variants of this approach including theories of the 'continuing crime'[84] and 'continuing elements' (where a crucial element of the offence is regarded as 'continuing' to take place in the jurisdiction, even if other elements take place without).[85] Another technique for overcoming the constraints of the territorial theory was to look for the "gist or kernel of the offence."[86] When elements of an offence are spread across different territories, the court prioritised one element, and location of that act was determinative.[87] Hirst equates this with the 'terminatory' theory,[88] despite Goode having previously convincingly argued that they are distinct tools of analysis. Goode's point is that when a court looks for the gist of an offence it considers the "purpose and objects of the offence",[89] not where the concluding act occurs.

Hirst proposes that the most revealing way of analysing and comprehending the range of seemingly divergent approaches in English law is to view them through the conduct and result crime dichotomy.[90] The consequences of an act are irrelevant to the former category, with the action itself being sufficient for criminal liability to be imposed.[91] Result crimes, on the other hand, criminalise behaviour only if it causes certain proscribed consequences.[92] Hirst may be correct that it is through the lens of this dichotomy that most sense can be made of the criminal laws of England and Wales in relation to cross-frontier crimes, but if he is, there is little hope of ever bringing this jurisprudence into coherence, for its analytical utility often ceases upon basic application of the distinction. As Goode notes, for many crimes the "'*exact*' distinction between

[83] See e.g. discussion of *R v Keyn* [1876] LR 2 Ex Div 63 in Ryngaert (2009), 191&194 for US examples.
[84] Goode (1997), 427-9.
[85] Ibid, 426-7.
[86] Hirst (2003), 118 quoting *R v Ellis* [1899] 1 QB 230.
[87] Goode (1997), 422.
[88] Hirst (2003), 118.
[89] Goode (1997), 426.
[90] Hirst (2003), 118.
[91] Ibid, 118.
[92] Ibid.

the two types of offence is not precisely clear",[93] and even Hirst admits that for some offences "the *actus reus* can take such a variety of forms that the orthodox view may become unworkable."[94]

The current approach of the English courts heeds, to some extent, this advice, and has "begun to move away from definitional obsessions and technical formulations aimed at finding a single situs of a crime by locating where the gist of the crime occurred or where it was completed."[95] The decision of Lord Woolf CJ in *Smith* remains the most authoritative statement of current practice, which recognises "jurisdiction if either the last act took place in England or a substantial part of the crime was committed here and there was no reason of comity why it should not be tried here."[96] This has been endorsed by the House of Lords,[97] and the 'substantial part' limb of this test applied in subsequent cases involving cybercrime, which will be discussed in chapter five. This additional limb adds substantially to the ambit of English criminal law, reflecting an inclusionary approach to territorial jurisdiction which has been neglected by scholars such as Ryngaert in their descriptions of the status quo. Nevertheless, the former limb testifies to the continued existence of the 'terminatory' theory, despite La Forest J's prediction of its demise.

While the English approach is critiqued for inconsistency and conservatism, the 'constituent elements' approach has its own troubles, being said to provide "few, if any, hurdles to even the most expansive assertions of competence."[98] It is often only the 'effects'-based variation of this approach which is highlighted as creating dangers to this end,[99] but it has long been recognised that even focusing on the 'elements' of a crime raises similar concerns.[100] As chapter five will demonstrate, however, the same criticisms can be levelled at interpretations of the 'terminatory' theory, at least as applied in the cybercrime context.

---

[93] Goode (1997), 437-8. Original emphasis.
[94] Hirst (2003), 128-9.
[95] *Libman v The Queen* [1985] 21 CCC (3d) 206, 221, *per* La Forest J.
[96] *Smith (Wallace Duncan) (No. 4)* [2004] QB 1418, [57].
[97] *Purdy v DPP* [2010] 1 AC 345, 370.
[98] Kohl (2007), 91.
[99] Parrish (2008), 1479, for example, argues that "[t]he effects test … gives license for near universal jurisdiction."
[100] Akehurst (1972-3), 155.

2.5 Extraterritorial Jurisdiction

It has been well documented that continental European countries are more willing to exercise extraterritorial jurisdiction (based on personality, protective or universality principles), than are their common law counterparts,[101] but even the latter countries have recently felt compelled to follow suit, taking a more expansive approach to extraterritorial jurisdiction,[102] due in part to the changing patterns of criminality associated with the globalisation of finance, travel, trade and telecommunications.[103] This has been done in a piecemeal *ad-hoc* fashion over particular offences, resulting in a "muddle" [104] and "mess" [105] of extraterritorial jurisdictional rules. Arnell even contends that the exceptions are "becoming so numerous so as to challenge the general rule [i.e. territorial jurisdiction]."[106]

The most common classification of extraterritorial grounds of criminal jurisdiction dates to the aforementioned ASIL study on jurisdiction, which identified four non-territorial grounds utilised by States, each of which will be considered in turn: nationality, passive personality, protection and universality.[107]

2.5.1. Nationality Jurisdiction

Nationality, also referred to as the "active personality principle",[108] provides States with the power to punish nationals [109] regardless of the place of commission of the offence. This is one of the most ancient grounds of jurisdiction [110] and is "universally conceded" [111] and apparently "hardly contested"[112] under international legal practice today. Such jurisdiction is said

[101] See Watson (1992), 46, Hirst (2003), 55 and Ryngaert (2008), 85 & 88.
[102] Hirst (2003), 45.
[103] Ibid, 59.
[104] Arnell (2001), 961
[105] Hirst (2003), 332.
[106] Arnell (2001), 961.
[107] Harvard Research (1935), 445.
[108] Ryngaert (2008), 88.
[109] State practice has now even stretched this to include domicile or residence. See e.g. s.12(4)(g) Bribery Act 2010 and Ryngaert (2008), 89 and Hirst (2003), 50.
[110] Watson (1992), 46.
[111] Akehurst (1972-3), 156. The authors of the Harvard study also referred to it as "universally accepted." Harvard Research (1935), 445. See further Hirst (2003), 50.
[112] Ryngaert (2008), 88.

to be "an attribute of sovereignty"[113] and based on the "allegiance which the person charged with the crime owes to the State of which he is a national."[114] Numerous explanations are found in the literature for this State power: the possibility of recidivism within the State;[115] the effect on the State's reputation by the conduct of its nationals abroad;[116] the protection of nationals abroad involving a reciprocal duty of obedience;[117] the prevention of impunity;[118] and "the impossibility of locating an offence."[119] As a result, some authors have recently called for an increased role for nationality jurisdiction, with Watson pleading in the US for a nationality-based criminal statute,[120] and Arnell, writing from the UK, calling for nationality to be placed "[along]side territoriality as a general basis of criminal jurisdiction."[121] They justify this on the basis of several factors: the international community's "collective interest in deterring crime";[122] the "lessened significance of borders"[123] given the ability of individuals to travel internationally and the fact that "technology has given rise to the ability to commit crimes remotely";[124] and the inadequacies of "the existing territorial jurisdictional scheme."[125]

From an enforcement perspective, these are pragmatic reasons for countenancing the nationality principle. However, Chehtman has offered a robust theoretical attack on this jurisdictional ground. His basic argument is that offences committed abroad do not bring into question the criminal law system of the national's State, and while knowing what the alleged offender did abroad may be repugnant to those within the State, "their belief in the system of criminal rules under which they live being in force is not undermined by these offences."[126] Arguments that point to the need to prevent impunity are critiqued for logically leading to universal jurisdiction, rather than

[113] Watson (1992), 64.
[114] Harvard Research (1935), 519.
[115] Chehtman (2010), 61.
[116] Harvard Research (1935), 519. See also Ryngaert (2008), 90, and Watson (1992), 68.
[117] Harvard Research (1935), 520. Watson (1992), 68.
[118] Watson (1992), 68.
[119] Ryngaert (2008), 90.
[120] Watson (1992), 83.
[121] Arnell (2001), 962.
[122] Watson (1992), 69.
[123] Arnell (2001), 959.
[124] Ibid.
[125] Ibid.
[126] Chehtman (2010), 61.

nationality.[127] Arguments that barriers to extradition justify nationality jurisdiction[128] confuse and conflate the power to punish with the power to refuse extradition, which are "logically independent from each other."[129]

Chehtman's abhorrence of the nationality principle is not an altogether new critique of State practice. For example, Stimson in 1936 regarded it as bad policy to base jurisdiction on this ground, arguing, like Chehtman, that "the government has no interest in the conduct of its citizens abroad except when that conduct results in injury to it, because the peace and good order of its territory is not disturbed."[130] Brenner, in the cybercrime context, also contends that nationality "seems to be a factor that militates against, rather than for, the assertion of jurisdiction",[131] and she proposes that "injured sovereigns should be given priority over the non-injured sovereign."[132]

2.5.2. Passive Personality

A ground of jurisdiction that is even more contested[133] in the literature is 'passive personality', which provides jurisdiction on the basis of the status of the victim. Whether this is a sufficient jurisdictional link under international law continues to be debated,[134] and is robustly critiqued in the literature on the grounds of infringing the principle of legality,[135] and increasing the risk of competency conflicts,[136] amongst others.[137] While some State practice appears to support this ground of jurisdiction in the context of terrorism offences,[138] it is not associated with any of the cybercrime offences found in the convention, and it will therefore not be discussed any further.

---

[127] Ibid, 61-3.
[128] See e.g. Watson (1992), 59-60.
[129] Chehtman (2010), 64.
[130] Stimson (1936), 1-2.
[131] Brenner (2006), 341.
[132] Ibid, 343.
[133] Watson (1992), 44. See further Harvard Research (1935), 579. Passive personality was not, as a result, included in the Draft Convention.
[134] Ryngaert (2008), 92.
[135] Ibid, 93. Moore (1887), 101 similarly critiques it for imposing an 'indefinite responsibility' on individuals, given the potential for the offender to be exposed to unforeseen prosecution by extraterritorial States, on the basis of the nationality of the victim in the territorial State.
[136] See Vabres (1928), quoted in Ryngaert (2008), 93. Mann (1964), 92 thus, contended it "should be treated as an excess of jurisdiction."
[137] See also Chehtman (2010), 67.
[138] Ryngaert (2008), 94.

2.5.3. The Protective Principle

The protective principle, on the other hand, is a more widely accepted extraterritorial ground of jurisdiction,[139] although uncertainty exists over the precise crimes to which it could relate. When one attempts to translate a principle which protects "sovereignty",[140] "territorial integrity",[141] "political independence"[142] or "State security"[143] into the proscription of certain conduct, it can be difficult to foresee precisely what is covered. Certain crimes, such as treason, espionage, counterfeiting of currency and government documents,[144] or computer-integrity crimes directed against State institutions, may easily be envisaged; others may not be as straightforward, since effects on State security may be an unintended consequence of the criminality. Akehurst therefore calls, as he does in his territorial 'effects' thesis, for the protective principle to be limited by a requirement that the "*primary* effect of the accused's action"[145] be the threatening of the State.

The protective principle is, however, rarely relied upon in practice,[146] which is particularly true in the criminal laws of England and Wales.[147] In the cybercrime context, the ease of accounting for incidents directed at State institutions within the territorial principle also suggests that it will serve neither to restrict nor to restrain jurisdictional assertions, even if more widely enumerated in criminal laws.

2.5.4. Universal Jurisdiction

The final extraterritorial ground of jurisdiction that is now sometimes said to have relevance in the cybercrime arena is universal jurisdiction. This allows every State to prosecute an offence, even if it cannot show any domestic impact or other jurisdictional nexus, in purported representation of the international community. The conduct must therefore shock the conscience of

[139] It is even embraced by Chehtman (2010), 69-70.
[140] Ryngaert (2008), 96.
[141] Harvard Research (1935), Article 7 of the Draft Convention.
[142] Ryngaert (2008), 96.
[143] Watson (1992), 43. Harvard Research (1935), Article 7 of the Draft Convention.
[144] Harvard Research (1935), Article 8 of the Draft Convention.
[145] Akehurst (1972-3), 159. Emphasis added.
[146] Ryngaert (2008), 98.
[147] Hirst (2003), 48 claims it is "not ... relied upon anywhere in English law."

mankind, and it is reserved for crimes of the most serious nature, being generally recognised to apply to the international crimes of genocide, war crimes, and crimes against humanity.[148] Piracy is the classic example of an international crime covered by universal jurisdiction,[149] and while cybercrime has been likened to traditional piracy, [150] the analogies would have to stop at the basic fact of criminal transgression of borders. [151]

Nevertheless, universal jurisdiction is increasingly being discussed in the context of cybercrime,[152] with many advocating its application.[153] Obokata, for example, calls for universal jurisdiction over transnational crimes given the widespread harm caused.[154] Cockayne, similarly speaks of an expectation of "substantive harmonisation"[155] of transnational offences such as cybercrime, which will result in an "organic growth of universal jurisdiction(s)."[156] Indeed, some States have even legislated to provide universal jurisdiction over certain categories of cybercrime, namely the distribution of child sexual abuse images.[157]

This fits a trend I will elaborate on in subsequent chapters, which sees the expansion of extraterritorial (and the meaning of 'territorial') jurisdiction to combat cybercrime as a necessity. Whether the expansion of jurisdictional bases is actually necessary, however, is a question which is seldom analysed, and in chapter five I demonstrate how the breadth of territorial jurisdiction suggests it is not; we are seeing a growth of near universal competence over cybercrime, but this must be distinguished from universal jurisdiction.

---

[148] See Bassiouni (2014), 416, Macado (2006), Olson (2011), 326 and Kreß (2006), 576.
[149] Harvard Research (1935), Article 9 of the Draft Convention. See also *Arrest Warrant (Democratic Republic of Congo v Belgium)* ICJ Reports 3 (2002), separate opinion of Judges Higgins, Kooijmans and Buergenthal, [61]-[63].
[150] Pinelli (2010), 501.
[151] Kreß (2006), 569 suggests that "[t]he *sui generis* characterization of piracy on the high seas as a crime of customary universal jurisdiction would seem to rest upon a combination of the absence of a territorial sovereign and the typical difficulty of establishing one of the traditional bases for alternative forms of jurisdiction such as, in particular, the nationality of the alleged offender." The problem with cybercrime is *locating* the perpetrator; territorial jurisdiction can normally be relied upon once this is established.
[152] Robinson (2006), 17.
[153] See e.g. Gable (2010) and Cottim (2010).
[154] Obokata (2010), 32 & 49.
[155] Cockayne (2005), 523.
[156] Ibid.
[157] Leslie (2014), 302, footnote 152.

Arnell is undoubtedly right to point to the dysfunctional nature of the territorial jurisdictional scheme, which rings particularly true with the advent of cybercrime. But this does not necessarily justify nationality[158] or universal jurisdiction.[159] The difficulty of determining who has the right to prosecute a criminal offence on a territorial basis does cry out for a simplistic solution such as a prioritisation of the State of nationality of the offender, but there are innumerable practical and theoretical difficulties with doing so. While there is little question of traditional extraterritorial grounds of jurisdiction supplanting territorial jurisdiction, there is an identifiable trend towards supplementing territoriality with extraterritorial principles in the cybercrime context.[160] This trend is likely only to exacerbate the difficulties associated with jurisdictional concurrency.

2.6 Resolving Concurrency?

The above has shown that international law has long recognised broad jurisdictional assertions by States, whether on territorial or extraterritorial grounds. While this may not have generated too many difficulties for States at the time of the ASIL's Harvard Research, scholars have begun to recognise that in today's globalising world, this internationally sanctioned system of concurrent jurisdiction now holds greater potential to generate problems for States, and unfairness for individuals.

Ryngaert contends that it is "only domestic courts' development of a second layer of norms applicable to transnational situations [which] might genuinely

---

[158] *Contra* Arnell, Hirst (2003), 332, suggests the "lessened significance of borders" and internationalisation of crime, "might more logically be used to argue in favour of a more flexible cross-frontier application of territorial principles, or perhaps for some use to be made of the protective principle."

[159] Calls for universal jurisdiction to deal with the cybercrimes found in the Convention also fail to appreciate the differences that exist with international crimes *stricto sensu,* where there is a greater level of agreement over the elements of the offences. In the former case, as Boister (2003), 958 notes, "[l]ittle or no attempt is made to define the fault element of the crimes to be enacted, which can result in very different domestic offences. The conduct elements of these crimes also suffer from definitional incoherence and ambiguity." Offences in this field can range from the trivial (logging in to someone's Facebook account) to the serious (compromising a large government database).

[160] See e.g. Directive on Attacks against Information Systems (Directive 2013/40/EU of 12 August 2013), Article 12(1)(b), and s.42(4) Serious Crimes Bill, which will amend the Computer Misuse Act 1990, to introduce nationality jurisdiction.

mitigate a State's jurisdictional assertions."[161] Below I discuss two proposals relating to such norm development.

2.6.1. The Principle of Legality

To deal with the heightened instances of jurisdictional concurrency, Luchtman[162] has attempted to draw on the principle of legality,[163] which is usually expressed in the maxims *nullum crimen sine lege* (no crime without law) and *nulla poena sine lege* (no punishment without law). This requires a level of precision in the drafting of criminal offences which "should contain *normative guidance* for the judge and for citizens."[164] It prohibits vaguely defined offences and retroactivity, and it has been argued that fair notice and the prevention of governmental abuse is at its core.[165]

While this principle is usually only understood to operate intra-States,[166] Luchtman contends "criminal law jurisdiction needs to be accessible and *foreseeable* to the individual"[167] so as to allow them to "predict *a priori* which particular state may claim jurisdiction."[168] Although he focuses on the operation of the principle within the EU, highlighting in particular the problems with unforeseeable exercises of extraterritorial jurisdiction and the need for this principle to operate within an area of free movement, his arguments are clearly capable of wider application.[169]

The potential application of traditional principles of criminal law to transnational crime cooperation is still an area in its infancy,[170] however, I am not convinced that the principle of legality will yield the results which Luchtman hopes for, and would be an impractical tool to apply as he proposes.

---

[161] Ryngaert (2008), 19.
[162] Luchtman (2012).
[163] For a comprehensive analysis of the principle see Gallant (2010).
[164] Krolikowski and Claes (2009), 107. Emphasis added.
[165] Luban (2010), 569.
[166] Although see May (2005), 109 for an analysis regarding international criminal tribunals.
[167] Luchtman (2012), 355. Emphasis added,
[168] Ibid, 358.
[169] Legality arguments have long been made relating to the operation of passive personality jurisdiction more generally: Moore (1887), 101.
[170] One exception within the EU is the principle of *ne bis in idem,* which will be discussed in my final chapter.

Expecting courts to assess what is 'reasonably foreseeable'[171] to the accused would add a considerable layer of complexity on top of existing jurisdictional conundrums, particularly as it would have to be weighed alongside the prosecutorial reasons for bringing the prosecution in the State concerned.

Moreover, in the particular context of the cybercrime offences addressed in the Convention, the principle would not appear to hold any greater potential for addressing concurrency. One of the reasons why agreement on the Convention was reached so quickly was because many States already had criminal laws pertaining to the offences concerned. The seriousness of the offences generally means that it is known that the behaviour is not legally innocent, and given that cybercriminals' activities will almost invariably engage numerous States' criminal laws, it is also reasonably foreseeable that the criminal laws of foreign States could be applicable.[172] The fact that States can usually also claim territorial jurisdiction over the offence makes it difficult to contend that there is any form of governmental abuse in a prosecution, as the State can show domestic effects.

2.6.2. Jurisdictional Reasonableness and Ryngaert's Rule of Reason

An alternative (judicial) norm for dealing with jurisdictional concurrency, and one that does actually feature in criminal cases with transnational elements,[173] is the concept of 'comity' or jurisdictional 'reasonableness'—that States should only extend and enforce their criminal laws if it is reasonable to do so, considering the interests of other States. While numerous principles of international law are supportive of this operating as a norm of customary international law (e.g. non-intervention), it has been argued convincingly that there is insufficient State practice and *opinio juris* for it to qualify as such: "[w]hen States exercise jurisdiction reasonably, they appear to do so as a matter of discretion, not out of legal obligation. Reasonableness, if any could

[171] Luchtman (2012), 371.
[172] It was observed in the *McKinnon* case that "[i]t must be obvious to any defendant that if you choose to commit a crime in a foreign country you run the risk of being prosecuted in that country." See *McKinnon* [2007] EWHC 762 (Admin), [33].
[173] See e.g. *Sheppard* [2010] EWCA Crim 65, [22].

be discerned, appears to be 'soft law' that need not guide future State behaviour as a matter of law."[174]

While acknowledging that the current system of jurisdiction is unsatisfactory, Ryngaert refuses to be "defeatist."[175] He proposes a "new theory of jurisdiction in international law":[176] drawing on the subsidiarity principle, he contends that States should apply their laws extraterritorially only if the State with the strongest nexus is unwilling or unable to deal with it. He hopes this abstract rule of reason will operationalise reasonableness and eliminate two problems with unilateral exercises of jurisdiction: the danger of pro-forum bias, and the lack of consideration of global interests.[177] Under this principle, all States are assumed to have an interest in clamping down on activities that are harmful to the international community,[178] and States with the strongest nexus or jurisdictional primacy would forfeit their right to protest if they have shown themselves unable or unwilling to deal with the harm at issue.[179] In the criminal law context, for example, territoriality is prioritised as a jurisdictional ground and only where the "territorial State fails to adequately prosecute the offender should other States be allowed to step in."[180] In terms of how this rule of reason will be put into practice, he draws on the work of Slaughter, and contends that a "*reasonable* exercise of jurisdiction could spontaneously spring from a network of transnational governance and judicial cooperation."[181] In other words, the exercise of jurisdiction becomes an act of networked governance, and before even contemplating the exercise of jurisdiction, States "should consult with relevant actors ... so as to be fully informed of foreign concerns over jurisdictional overreaching."[182]

There are three main reasons why this rather utopian jurisdictional framework will be unlikely to solve the difficulties with concurrency, particularly in the

[174] Ryngaert (2008), 178.
[175] Ibid, 182.
[176] Ibid, 185.
[177] Ibid, 184.
[178] Ibid, 214.
[179] Ibid, 215.
[180] Ibid, 218. Bassiouni (2014), 378 in his analysis of jurisdictional concurrency also suggests a prioritisation of the territorial principle.
[181] Ibid, 211.
[182] Ibid, 185.

cybercrime enforcement. First, and most obviously, a prioritisation of territoriality will do little to assist in this context because, as has been mentioned, the main problem lies in determining a 'primary' territorial State. Second, his rule of reason would require State actors to pass judgment on other States' willingness or ability to prosecute an offence. He acknowledges that this is "anathema to a State-centred conception of international law",[183] but he under-appreciates how this could actually engender further conflict between States, as their courts and transgovernmental actors cast judgment on one another. Moreover, the idea that States are under a 'duty' to positively assert jurisdiction over cybercrime[184] is unlikely to gather traction, as it would be seen to interfere with States' independence in controlling domestic affairs. Third, Ryngaert's theory may place too much faith in the abilities of transgovernmental networks to resolve the cooperation difficulties generated by globalisation, and to further an ill-defined 'global interest.' As Verdier has argued, there are multifaceted domestic constraints on networking actors who are simply not "free to disregard domestic preferences in their states and pursue globally optimal policies."[185] In chapter six, I will elaborate on these constraints drawing on my interviews with cybercrime investigators and prosecutors. Therefore, while there have been some notable attempts to address jurisdictional concurrency in the literature, none would appear equipped to deal with the phenomenon of cybercrime.

2.7 Conclusion

In the 19th century it was said that a State possesses and exercises "exclusive sovereignty and jurisdiction throughout the full extent of its territory [and that] no State can, by its laws, directly affect, bind, or regulate property beyond its own territory, or control persons who do not reside within it."[186] This was an

[183] Ibid, 216.
[184] Ibid, 36. Ryngaert claims that "[s]overeignty should no longer be an excuse or a shield, but a responsibility: every sovereign nation has a responsibility not to condone or encourage activities that are, from a global perspective, harmful." Ibid, 186.
[185] Verdier (2009), 126.
[186] Wheaton (1866), section 78.

overstatement even then,[187] as territoriality has "never [been] a hard and fast rule."[188] States now increasingly prescribe and assert extraterritorial criminal jurisdiction, and this is also becoming a common trend in the cybercrime context,[189] despite being jurisprudentially questionable in some of its most prominent forms (e.g. nationality). Territoriality itself, as a legal construct, is unstable and is constantly undergoing transformation,[190] as the various approaches to trans-jurisdictional offences outlined above demonstrate. Chapters five and seven will demonstrate how this has allowed for the most expansive of jurisdictional claims, with States sometimes prosecuting individuals on the basis of little more than the accessibility of content within its territory. This, as noted in the introduction, is an insidious development. In the next chapter I will explain why—and how—States largely forego their ability to complain about many unilateral seizures of jurisdiction when they ratify conventions with permissive extraterritorial grounds. Multilateralism is called for because it is thought to prevent "unorthodox unilateral practices"[191] and while it has long been recognised that assertions of extraterritorial jurisdiction can hamper international relations and cooperation,[192] it is the concept of territoriality over cybercriminality that should be the greater concern. Raustiala writes about "Empire and extraterritoriality in 20th Century America."[193] But in 21st Century America we will write simply of empire and territoriality—the orthodox unilateral practice. Moreover, while concurrency has long been envisaged in international law, the problem is clearly more pronounced in the information age. There is, as Bassiouni notes, "very little international law to resolve such conflicts"[194] and recent suggested frameworks have been argued above to be impractical (Luchtman) or ill-equipped to deal with the complexity of cybercrime (Ryngaert). However, Ryngaert's work has highlighted the fact that it is within TGNs where the place of prosecution can be determined, and

[187] As Raustiala (2005), 2510 notes, "the ideal of Westphalian territorial sovereignty was riddled with exceptions from the beginning", giving the example of universal jurisdiction over piracy.
[188] Ibid, 2510.
[189] See chapter five.
[190] Sassen (2013), 24.
[191] Gilmore (1992), 1556.
[192] Blakesley (2008), 1109. See also Ryngaert (2008), 188 and Gibney (1996).
[193] Raustiala (2011).
[194] Bassiouni (2014), 415.

the drafters of the Convention similarly expect that concurrency should be addressed here. The practicalities, consequences, and risks with this, will be explored in chapters six to eight.

The concept of territoriality is also undergoing considerable change in the realm of enforcement jurisdiction, as States simultaneously relinquish the sorts of strict territorial control envisaged in *Lotus*, while expanding the power of their domestic LEAs. Raustiala has argued that "[a]s technology evolves, legal spatiality becomes harder to apply and harder to justify as a jurisprudential principle."[195] The trajectories that I will be describing in the realms of enforcement jurisdiction, and the jurisdiction to prescribe, provide ample ground for agreeing with this assessment. And as the next two chapters demonstrate, the Convention is a considerable driver in these territorial conundrums, with considerable efforts also underway within the Council of Europe to further expand enforcement powers, which would further transform concepts of territoriality. This trajectory will be critiqued in chapter four, before I combine this analysis with my problematisation of jurisdictional concurrency in remaining chapters, thus providing a holistic picture of the Convention and what may lay in store in its operation. First, however, more must be said about the suppression process, which is the subject of the next chapter.

[195] Raustiala (2005), 2513.

Chapter 3: The Suppression Process

"We are compelled by the globalization of crime to globalize law and law enforcement."[1]

"Multilateralism is our shared secular religion."[2]

3.1 Introduction

Over the last century, whenever new forms of transnational criminality have arisen, States have typically turned to, and indeed have been expected to turn to,[3] suppression conventions: international agreements where States agree to mutually suppress a particular form of criminality.[4] This chapter explores these instruments as one of the most important processes through which States have responded to the globalisation of crime.

The purpose of this chapter is to place the Cybercrime Convention in context, so as to explain its current structure, and the motivations and concerns that will likely drive its development. I begin with an explanation of some of the key terms used in this chapter, and some of the different processes that are relevant to my thesis. Section three explains the motivations for creating suppression conventions, and the reasons for certain constructs within them, while my fourth section outlines some of the historical patterns that can be seen across these conventions. Finally, section five recounts the processes behind the Convention, and briefly describes its main provisions. It is argued that the Convention has followed the conventional pattern of such instruments; it is almost myopic in focusing only on means for improving transnational access to

[1] Kerry (1997), 169.
[2] Alvarez (2000), 394.
[3] Gilmore (1992), 1554 claims that "[t]here is an obvious, some would say compelling, need for consideration to be given to extending the types of obligation contained in the 1988 UN Convention in such areas as mutual assistance and confiscation of proceeds so as to embrace other serious non drug specific offences." Likewise, Soukieh (2011), 223 states that "[j]urisdictional issues will continue to frustrate cybercrime investigations and prosecutions at every level, until all core stakeholders begin to see international treaties, not as a devaluing of national sovereignty, but as a pre-requisite to international trade and security."
[4] Boister (2012), 14. Nadelmann (1990), on the other hand, refers to "global prohibition regimes." However, his term is descriptive of broader phenomena, beyond international conventions alone. Since I am primarily interested in the mechanics of the Cybercrime Convention, I will therefore adopt Boister's term "suppression conventions."

information and criminals, and adopts standard jurisdictional provisions. This fails to appreciate, or address, any of the implications of jurisdictional concurrency in cybercrime, and the scale of the emergent difficulties results in something of an imbalance in the Convention.

3.2 Transnational Criminal Law

In order to understand why States have sought to address cybercrime within the Convention, it must be placed in context as a particular form of criminality within international law. It is clearly a 'transnational crime', but this is a term often used to describe very different phenomena. Frequently, when governments and academics speak of transnational crime, they are referring to transnational *organised* crime,[5] which itself comes with a variety of labels and descriptions.[6] On other occasions transnational crime is conflated with international crimes, the latter referring to crimes which are *delicta juris gentium,* or of concern to the international community as a whole.

It has been suggested[7] that a very basic way of distinguishing between these crimes is that international crimes can be committed exclusively within one State, whereas transnational crime, by its very description,[8] would appear to always involve trans-boundary effects. This distinction, in isolation, is insufficient,[9] for most offences regarded as transnational crimes can also be committed exclusively within one State. Boister has more clearly distinguished between international crimes *stricto sensu,* and, what he has coined, transnational criminal law (**TCL**). The latter involves "the indirect suppression by international law through domestic penal law of criminal activities that have actual or potential trans-boundary effects."[10] While core international crimes[11]

[5] Giraldo and Trinkunas (2009), 431.
[6] Obokata (2010), 13.
[7] Ibid, 31.
[8] Passas (1999), introduction, xiii-xiv: "Crime becomes transnational when victims are located in, or operate through, more than one country." See further Natarajan (2011), introduction xxv: "transnational crimes are criminal acts or transactions that span national borders, thus violating the laws of more than one country." See also Article 3(2) of the Convention Against Transnational Organized Crime (2225 UNTS no. 39574, New York, 2000), (the **UNTOC**).
[9] Obokata (2010), 32.
[10] Boister (2003), 955.
[11] On the elements of international crimes, see Cryer (2005), chapter five and Cryer and Bekou (2007). See further Bassiouni (2012).

can carry international criminal liability regardless of domestic legislation, "[a] transnational crime like drug trafficking may find its original normative source in international law, but the actual criminal prohibition on individuals is entirely national."[12] TCL, therefore, only applies to those offences that have been found by States to have necessitated a "suppression convention",[13] an international agreement by States to suppress transnational crimes. It is a category that does broadly relate to international criminal law and they share similarities: both can refer to inter-State and intra-State criminal activity, both can involve domestic criminal law with international law roots, and both reflect "shared interests of cosmopolitan values"[14] (although the level of consensus is greater for core international crimes). However, they are distinguishable.

The *modus operandi* for suppressing the specified activity in these conventions is now normally two-fold: first, to facilitate the domestic suppression of the activity (whether intra-State, or inter-State[15]) by defining minimum elements for criminal offences (harmonisation), which must be adopted by each State Party, and requiring the creation of investigative procedural powers; second, to enable inter-State action through a variety of cooperation mechanisms. The former has essentially attempted a "*homogenization* of criminal justice systems."[16] The latter has also entailed "the *regularization* of criminal justice relationships across borders." [17] Suppression conventions, such as the Cybercrime Convention, are one of the primary tools used by States to realise these goals: the harmonisation of cybercrime offences not only assists in suppressing cybercrime by allowing domestic prosecutions, but it also facilitates co-operation with other countries by ensuring dual criminality.

My thesis centres on the operation of these dual objectives in the context of the Convention. However, the multiplicity of arrangements to which States are subject in the fight against transnational crime, require that I also note broader developments, even if these are not the primary *situ* of my research. For

[12] Boister (2012), 19.
[13] Ibid, 14.
[14] Boister (2003), 968.
[15] This is because of the tendency of intra-State crime to lead to inter-State crime. See Boister (2012), 15.
[16] Andreas and Nadelmann (2006), 8. Original emphasis.
[17] Ibid.

example, while suppression conventions can form the basis upon which States interact in the movement of evidence,[18] or even people,[19] in many instances, bilateral treaties or other forms of arrangements supersede the Convention and govern such interaction.[20] For this reason, a regional development that cannot be ignored is the EU.

3.2.1. Regularisation of Relationships in the EU

The EU is assuming an increasing role in both the harmonisation of cybercrime laws[21] and improving inter-State processes and criminal justice relationships to enforce them. Few would have envisaged any role for the EU in matters of domestic criminal law until the Treaty of Maastricht in 1992. Such has been the pace of development in this sphere since then that entire books are now written about EU criminal law.[22] Cooperation between EU Member States has been completely transformed in recent years, based on the concept of "mutual recognition."[23] This has considerably expedited cooperation in relation to the movement of evidence[24] and suspects[25] because, unlike the procedural dimensions of suppression conventions which follow a "request model", the mutual recognition instruments adopt a "command model."[26]

While analysis of these procedural instruments is beyond the scope of this thesis, I will be considering the role of two EU agencies: Europol and

[18] See e.g. Article 27(1) of the Cybercrime Convention.
[19] See e.g. Article 24(3) of the Cybercrime Convention.
[20] For example, the extradition of a cybercrime suspect between the US and the UK will be governed by their bilateral treaty, rather than by provisions of the Cybercrime Convention.
[21] See e.g. the Directive on Attacks Against Information Systems (2013/40/EU, 12 August 2013). For discussion of this development see e.g. Walden (2004).
[22] See e.g. Klip (2012) and Mitsilegas (2009).
[23] Mitsilegas (2009), 101 explains it as follows: "[m]utual recognition entails the acceptance of judgments issued by *national* criminal courts, reflecting their domestic criminal justice systems. A court in the executing Member State is under the obligation to recognise and execute the judgment from its counterpart in the issuing Member State with the minimum of formality and with limited grounds of refusal."
[24] See the European Investigation Order (Directive 2014/41/EU, 3 April 2014). This allows investigating authorities to request, *inter alia,* that other States intercept communications in the Member State from which technical assistance is needed (Article 30-31) and provide for the collection of traffic data associated with telecommunications (recital 30 of the Directive). This will significantly empower cybercrime and other criminal investigators within the EU.
[25] See the operation of the European Arrest Warrant (Council Framework Decision 2002/584/JHA, 13 June 2002).
[26] Spencer (2013), 63.

Eurojust.[27] Both are significant reasons why Europe is "the region of the world where cross-border law enforcement relations are the most intensive, advanced, and institutionalized."[28]

Cooperation between European police forces has a long history,[29] and within the European Community, informal structures date from at least the 1970s.[30] The Maastricht Treaty was pivotal in institutionalising a formal European Police Office,[31] with a Europol Convention agreed in 1995, and coming into force in 1998.[32] Although Europol has no powers of arrest, or of using coercive measures, it operates as a vital hub in the exchange and analysis of information in relation to serious crime within Europe Member States, and sometimes even beyond.[33] In 2013, a European Cybercrime Centre (**EC3**) was also established within Europol, with the aim of, *inter alia,* supporting cybercrime investigations within the EU, facilitating cooperation with third States, and coordinating complex transnational investigations. Europol and EC3 can, therefore, assume a much wider role than the information exchange forum which Europol was initially envisaged to be, and can, acting through the Director of Europol, even request that Member States initiate investigations.[34] These powers will be considered in chapter six.

Eurojust, on the other hand, was established later in 2002,[35] and is a network of prosecutors, judges or police officers of equivalent competence, seconded by each Member State, who in the context of investigations and prosecutions of

---

[27] The Commission referred to Eurojust and Europol as agencies in one of their communications to the European Parliament and Council: "The Way Forward" COM (2008) 135.
[28] Andreas and Nadelmann (2006), 223.
[29] For an excellent historical overview, see Andreas and Nadelmann (2006) 59-104, and see also Hufnagel (2013), chapter two, Fijnaut (1993) and Hufnagel and McCartney (2014).
[30] See Bunyan (1993).
[31] Article K1 of the Treaty on European Union (Maastricht, 1992).
[32] The Convention, and its three Protocols, were eventually replaced by the Europol Decision (Council Decision 2009/371/JHA, 6 April 2000), (the **Europol Decision**).
[33] It must, however, have agreed operational or strategic agreements for these purposes with third States and organisations. See Article 23 of the Europol Decision. It currently has operational agreements with eleven countries, which can include the exchange of personal data of suspects between LEAs. See https://www.europol.europa.eu/content/page/external-cooperation-31 (Accessed 20/12/2014). See also chapter four, section 4.4, on the role of liaison officers in Europol.
[34] See Article 7 of the Europol Decision, *supra* note 32.
[35] Eurojust Decision (Council Decision 2002/187/JHA, 28 February 2002). The decision was amended by Council Decisions 2003/659/JHA and 2009/426/JHA. See now the consolidated version 5347/3/09 COPEN 9 EUROJUST 3 EJN 2, (the **Eurojust Decision).**

serious crimes concerning two or more Member States, support one another in coordination, and in improving cooperation by facilitating the execution of requests. Eurojust is, therefore, the judicial counterpart to Europol, although since both can assist in the coordination of investigations, the lines can sometimes be blurred.[36]

Despite the focus of this work being on the Convention, the work of these agencies will be considered in subsequent chapters for the following reasons. First, both are crucial hubs for the work of TGNs and for facilitating many of the procedural aspects of suppression conventions, both between EU countries, and beyond.[37] Cybercrime Convention provisions that ask countries to exchange information, or provide MLA, will often be enabled and expedited through these agencies. Second, both can be crucial focal points for jurisdictional negotiations in cybercrime cases, again between EU countries as well beyond, and Eurojust is the only organisation to have produced guidelines for the conduct of such negotiations.[38] Therefore, these agencies can be crucial cogs in the way States comply with many provisions of the Cybercrime Convention. Finally, awareness of forms of cooperation between EU countries can assist in imagining how cooperation may develop in instruments like the Cybercrime Convention. As Boister notes, "Europe has become a laboratory for the development of other cross-border forms of cooperation."[39] While certain concepts within EU criminal justice cooperation, such as mutual recognition, are unlikely to be adopted more broadly,[40] the Union's approach to

[36] The idea that Eurojust deals with coordination at 'judicial' level, while Europol deals with it at 'police' level, assumes a clear line can be drawn as to when investigations move from being police, to prosecutorial issues. Within the UK, however, prosecutors are often involved from an early stage in investigations, particularly involving transnational cybercrime investigations. The overlap is also demonstrated by the fact that prosecutors often attend meetings at Europol, and each agency frequently attends coordination meetings in its counter-part.

[37] See e.g. chapter four, section 4.4, and the growing number of liaison officers situated in Europol.

[38] See chapter six.

[39] Boister (2012), 165. See also Andreas and Nadelmann (2006), 240 on the role of the EU shaping the direction of international law enforcement developments.

[40] This is particularly because there are serious concerns with the operation of the mutual recognition principle, even between EU countries, since it artificially equates the free movement of goods, with the free movement of judgments and prioritises the country of first initiative. See Peers (2004), 24, Spencer (2013), 65 and Klip (2012), 393. As Klip (2012), 392 notes, "[t]he emergence of all manner of orders (arrest, evidence, execution) rides roughshod over consultations with other parties."

ne bis in idem, for example, does have greater potential for wider adoption and will be discussed in chapter eight.

3.3 The Formation of Suppression Conventions

The 21st century has seen an explosion of multilateral treaties,[41] with suppression conventions very much in keeping with the trend. A burgeoning area of international law scholarship in recent years has attempted to theorise why States enter into these binding international treaties, rather than non-binding pledges or agreements.

One of the most comprehensive explanations for why States enter into treaties is Andrew Guzman's "rational choice theory."[42] Guzman draws on well-known contractual theories and game theory to explain treaty formation. He contends that:

> …states enter into treaties for the same basic reasons that individuals enter into contracts. Treaties allow them to resolve problems of cooperation, to commit to a particular course of conduct, and to gain assurances regarding what other states will do in the future.[43]

His baseline analytical assumptions are clearly laid out: "States are assumed to be rational, self-interested, and able to identify and pursue their interests."[44] States are therefore treated as black boxes, divorced from domestic groups and actors (or capable of being understood without them), and rational, in that they are only interested in maximising "their own gains and payoffs."[45] In Guzman's model, States will only enter into treaties if they will experience some gain, "and that gain must be larger than what they invest."[46]

A crucial concern for States in deciding whether to agree treaties is their enforceability,[47] and the likelihood of compliance by other States. Short-term payoffs from breaching obligations under a treaty can sometimes outweigh the

[41] See for example the analysis by Denemark and Hoffmann (2008), 188 of a huge dataset of 6976 multilateral treaties signed between 1595-1995, noting a particular escalation in the last century. See also the COIL dataset: Koremenos (2013).
[42] Guzman (2008).
[43] Ibid, 121.
[44] Ibid, 17.
[45] Ibid.
[46] Ibid, 12.
[47] See e.g. the weak dispute settlement provisions of the Cybercrime Convention, Article 45.

payoffs from cooperation. Guzman points to the 'three R's' which elucidate the reasons for compliance: retaliation, reciprocity, and reputation. Following non-compliance by a State, other States may retaliate, may reciprocate the violation, or may not cooperate in the future given its reputation for non-compliance.[48] As Guzman explains in his earlier work, a treaty is therefore a "double-edged sword [in that it] generates higher levels of compliance which (assuming the parties select the terms optimally) increase the joint payoff, but in the event of a violation it imposes a larger penalty on the violating state"[49] (in the form of reputational harm). The desire of States to increase the credibility of commitments is thus tempered by the competing goal of avoiding such reputational loss. The benefits for the parties from increased compliance must outweigh the potential imposition of costly sanctions, which are more likely when an agreement assumes a 'hard' form, like a treaty.

This model also allows Guzman to make certain predictions as to when treaties are more likely to be utilised. First, when reputation is unlikely to affect decisions (e.g. because the substantive issue at play involves a question about a State's sheer existence), credibility-enhancing mechanisms are unlikely to be used. 'Low stakes' issues are, therefore, more likely to be the subject of treaties.[50] Another consequence of his model is that when the probability of violation is small, treaties are more attractive options (since the costs are only felt when the treaty obligations are breached.)[51] As the possibility of violations decreases, the likely value of the treaty increases. A final element worth noting is his approach to what Raustiala has called, the "substance of an agreement."[52] This refers not to the subject of the agreement, but to the "depth or shallowness of the commitments."[53] Guzman quotes Downs, Rocke, and Barsoom who define depth as "the extent to which [an agreement] requires states to depart from what they would have done in its absence."[54] In other words, some substantive provisions may require little change from the status quo, while

[48] Ibid, 30-32.
[49] Guzman (2005), 597.
[50] Ibid, 605.
[51] Ibid, 606.
[52] Raustiala (2005), 601.
[53] Ibid.
[54] Downs, Rocke, and Barsoom (1996), 383.

'deep' provisions would do so. Guzman predicts that States, when drafting an agreement, will balance the desire to make effective and efficient commitments against the desire to avoid reputational harm in the event of breach. He suggests that States may therefore "select substantive terms that are systematically weaker than those that would maximize the benefits to the states if a costless (i.e. zero sum) system of damages were available."[55] This conclusion is in keeping even with scholars who eschew game theory and functionalist accounts.[56] A related issue, dissected in some detail by Guzman, is the role uncertainty plays in assessing compliance and reputational harm: if an action isn't clearly a breach of a treaty due to the performance standard being uncertain, then the risk of reputational harm will be reduced.[57]

3.3.1. Critiques of Guzman

Guzman does not deny that other theories can have explanatory force,[58] but nevertheless makes claims as to the theory's universality,[59] and that it offers greater predictive potential than other theories.[60] The boldness of these assertions has naturally prompted critiques, from a variety of angles. Geisinger and Stein, for example, argue that his theory insufficiently captures the role which reputation plays in treaty formation,[61] while Brewster challenges his account of reputation from a different angle, questioning, *inter alia,* the extent to which it actually constrains State conduct.[62] Kydd, on the other hand, points

[55] Guzman (2005), 603. Sanctions have a zero sum character e.g. in the domestic context, where a contractual breach will result in the breaching party paying damages to the other; what is lost by one, is gained by the other. The sanctions of treaty breach do not normally have this character; the breaching party suffers reputational harm, but the other party does not enjoy offsetting gain. Ibid, 581-2. Other States capture the reputational loss—not only those that are parties to the agreement—in their knowledge of a Party's reputation for breaching its commitments. Ibid, 596.
[56] See e.g. Raustiala (2005), 601 who argues "[t]he more shallow the commitment, the more likely performance will be, and therefore the more credible the commitment ex ante. Negotiating commitments as contracts should lead to a reduction in the depth of those commitments."
[57] Guzman (2008), 97.
[58] Ibid, 18-22.
[59] Ibid, 121-2.
[60] Ibid, 21.
[61] Geisinger and Stein (2008).
[62] Brewster (2009). Most of these concerns did, however, appear to have been addressed in his book. See Guzman (2009), 335-338.

to the importance of domestic politics in influencing international conduct[63] while Peterson, in similar vein, claims that Guzman's theory cannot holistically elucidate how international law works because it has a blind spot – preferences.[64] 'Rational choice' cannot explain the formation of preferences, or why they change, yet Guzman's model depends on the prediction of preferences. Peterson admits, however, that where one can observe stable preferences in the past, and where there have been numerous interactions, this challenge may not be insurmountable: "if you can make relatively stable assumptions about the preferences of the relevant actors and if you want to explain why actors choose a specific strategy, then rational choice provides the best analytical instruments."[65]

3.3.2. Rational Choice and Suppression Conventions

Guzman may have to succumb to some of these critiques,[66] but his 'Rational Choice' theory is, by and large, a compelling and convincing theory of treaty formation and compliance. In particular, I believe it explains much about suppression conventions. The gains that States make from their engagement with the international community are fairly readily comprehensible in this regard. Suppression conventions do not just deal with any crimes (even crimes which are universally sanctioned such as murder and rape); they deal with *transnational* crimes. As transnational crime globalised, unilateral and even bilateral law enforcement measures were quickly shown to be inadequate. Given the strict territorial nature of States' enforcement powers, the investigation and prosecution of transnational crime—a concern for all organised societies—became a more challenging endeavour. This goal could

[63] Kydd (2009). See also Raustiala (2005), 595. Again, however, Guzman seemed fully aware that the assumption of unitary states is simplistic, but he justified this model because "despite progress made on the question of how domestic politics influences international conduct, we lack a satisfactory model of domestic politics that would allow the development of a general theory of international law." Guzman (2009), 338.
[64] Peterson (2009), 1258. See also Engel (2005).
[65] Peterson (2009), 1260.
[66] I find the critique by Geisinger and Stein (2008) particularly compelling. However, it is relevant only to instruments that do not provide the types of cooperative benefits upon which Guzman conditions treaty formation, e.g. a State that favours using child labour agreeing to stop doing so. With suppression conventions, there are direct material benefits for all States involved.

no longer "realistically be confined within national boundaries",[67] and this was particularly true within the EU after the opening of borders pursuant to the Maastricht Treaty.[68] The suspects inflicting domestic harm, and evidence in relation to it, were often based abroad, and gaining access to either was often hampered by issues such as the idiosyncrasies of legal systems, diverging methods of evidence collection, language, etc. Rational, self-interested actors had to cooperate together in order to increase their respective individual welfare. Suppression conventions were "intended to minimize and even eliminate the potential havens from which certain crimes can be committed and to which criminals can flee to escape prosecution and punishment."[69] As mentioned, they did so with a two-fold strategy: homogenising criminal justice systems so as to incentivise domestic suppression of the particular criminality, and enabling international cooperation.

In some of the earlier suppression conventions, the costs were greater for some. Britain, for example, was the principal sponsor of the opium trade until very late into the 19th century, once generating substantial revenues from opium exports between British India and China,[70] and it required an aggressive campaign against the trade—primarily from actors in the US—to stimulate the creation of suppression conventions. Generally speaking, however, States do not directly benefit from the activities suppressed in these conventions,[71] and the costs in this first limb are limited to, for example, the actual economic costs of domestic law making and the creation of procedural powers and specialised units within law enforcement to deal with the activity. In return, the multilateral nature of the endeavour provides many benefits, particularly when there is "transnational moral consensus regarding the evil of a particular

[67] *USA v Cotroni* [1989] 1 SCR 1469, 1470.
[68] Spencer (2013), 66.
[69] Andreas and Nadelmann (2006), 19.
[70] Ibid, 39.
[71] There are, however, exceptions to this. A Grand Jury in Pennsylvania recently indicted five members of the Chinese military for hacking into American computer systems. See *US v Dong and others* (Western District of Pennsylvania Indictment, Criminal no. 14-118, 1 May 2014). The Director of the FBI stated after the indictment was unsealed, that "the Chinese government has blatantly sought to use cyber espionage to obtain economic advantage for its state-owned industries." See http://www.fbi.gov/pittsburgh/press-releases/2014/u.s.-charges-five-chinese-military-hackers-with-cyber-espionage-against-u.s.-corporations-and-a-labor-organization-for-commercial-advantage (Accessed 20/12/2014).

activity."[72] With each State suppressing the activity within its territory, the likelihood of that particular harm affecting a particular country is substantially reduced, and the costs of law enforcement are also externalised. As the Supreme Court of Canada has noted, "[i]n a shrinking world, we are all our brother's keepers."[73]

Married to the provisions dealing with domestic suppression of the activity was (particularly in later conventions) a procedural regime designed to facilitate inter-State cooperation in various respects (the second limb of the suppression strategy). During the latter half of the 19th century many States were fast developing experience with bilateral extradition treaties, while the 20th century saw a similar development of experience in areas like MLA. Provisions relating to both gradually made their way into suppression conventions. As Boister notes, "[e]xperience with general MLATs resulted in the inclusion of mini-MLATs within more recent suppression conventions."[74] The former limb enabled much of this procedural interaction, by ensuring dual criminality.

The costs and benefits of these procedural provisions, however, were often a more delicate point of negotiation. Civil law countries were reluctant to extradite their nationals. Jurisdictions like Switzerland were keen to protect their reputation for banking secrecy and reluctant to agree to MLA provisions that would jeopardise this. Indeed, after a bilateral MLAT between the US and Switzerland in 1976, other countries, such as Austria and Liechtenstein, began to tout themselves as safer financial security jurisdictions.[75] But the reciprocal nature of these agreements had wide appeal. While States recognised that they would have to invest substantial resources in responding to various requests from other counties, in exchange, their domestic criminal investigations would not be hampered due to factors such as the location of evidence or suspects. Moreover, having experience with bilateral mechanisms of a similar nature, the costs of creating institutions for responding to these requests were minimal. And because they had seen the operation of these procedural measures in

[72] Andreas and Nadelmann (2006), 228.
[73] *Libman v Queen* [1985] 2 SCR 178, 214.
[74] Boister (2012), 199. MLAT refers to a Mutual Legal Assistance Treaty.
[75] Nadelmann (1993), 344. For an analysis of the negotiations regarding this treaty see ibid, 324-341.

bilateral treaties,[76] they could predict that their violations would be infrequent, which thus reduced the expected reputational risks of the treaty. This was also achieved by maintaining shallowness in their commitments.

The ratification of these conventions will clearly be more onerous for some more than others. Many countries already have the requisite infrastructure and laws in place long before the negotiation of the suppression convention even begins.[77] The US, in particular, has seldom had to accommodate the wishes of other countries in this sphere. As Friman has noted, "the United States continues to dominate the structure and normative content of global prohibition regimes."[78] On the other hand, some countries might only suffer marginally from the proscribed activity and may thus be reluctant to ratify such a convention. However, the aforementioned reciprocal benefits carry much weight. Some additional benefits and motivations for agreeing suppression conventions that are noteworthy include: the reluctance of States to be seen as safe havens for criminality;[79] the desire to prevent other countries from exercising enforcement powers within their territories;[80] the difficulty of assessing the magnitude of the threat faced from the proscribed activity; the categorisation of the activity as a national security threat;[81] and even the desire of States to mask the imbalance in their relationships with powerful countries, by portraying their activities (e.g. the extradition of their nationals) as in

[76] The disadvantage of a multilateral convention over bilateral arrangements, as Nadelmann (1993), 9 notes, is that it cannot accommodate the mutual peculiarities and preferences of two countries, and must "settle for the typically low level of accommodation required to win the adherence of a diversity of states." The advantage, on the other hand, was it reduced the need to negotiate multiple bilateral agreements, the (economic) costs of which could be significant.

[77] See e.g. the case of the UK and its ratification of the Cybercrime Convention in 2011; no substantive legal changes were required.

[78] Quoted in Andreas and Nadelmann (2006), 244. See e.g. the OECD Anti-Bribery Convention, (37 ILM 1, 1998), which was based substantially on the US Foreign Corrupt Practices Act 1977. Boister (2012), 18.

[79] According to Geisinger and Stein (2008), 1137 this sort of reputational factor cannot be accounted for in Guzman's theory as "reputational forces become relevant only after a state's legal obligations exist. … Put a different way, failure to join a treaty would have no reputational consequences within the Rational Choice framework."

[80] This is a particular problem with exercises of US enforcement powers: Andreas and Nadelmann (2006), 314.

[81] This is particularly true for cybercrime. For example, the UK's 'National Security Strategy' (London, 2011) categorised cyber attacks as a tier one threat to national security.

compliance with international duties.[82]

When all of these factors are combined, it is clear how resort to suppression conventions became almost self-evident, and the 'rational choice.' States began to "worship at the shrine"[83] of such initiatives. My next section describes some of the patterns in the evolution of suppression conventions, and demonstrates how certain provisions began to be transplanted almost pro-forma, while other provisions were expanded to take account of new threats. This, I argue, serves to explain much about the structure of the Cybercrime Convention, and how aspects of the instrument may not have received adequate attention in negotiations.[84] The depth of these agreements increased, barriers to cooperation were gradually removed, and provisions that were not causing difficulties in other contexts (such as jurisdictional provisions) were transposed almost verbatim. But it seems that the perceived self-evident utility of such conventions reduced the rigor of analysis en route. As Klip notes in the context of the EU: "[i]t is striking how little the question of the need for the integration and harmonisation of criminal law comes up in discussions within the Union."[85] I contend, in particular, that the jurisdictional implications of the Cybercrime Convention were not appreciated, and that they will have (and are having) unforeseen consequences.

3.4 The Pattern of Suppression Conventions

While there is a vast literature on the genesis of some suppression conventions, particularly those pertaining to drug trafficking—which was one of the key catalysts for these conventions developing[86]—there is little in terms of systematic historical analysis across the suppression conventions, and some of

[82] Andreas and Nadelmann (2006), 243. Conversely, the US can use these conventions to exercise their policing hegemony without resorting to internationally unlawful activities.
[83] Alvarez (2000), 394.
[84] See also Nadelmann (1993), 458 in the context of extradition treaties, on how extradition treaties are no longer "negotiated with a keen sense of their intended limits…" This rings equally true in the context of suppression conventions.
[85] Klip (2012), 24.
[86] See e.g. Lowes (1966), Anslinger and Tompkins (1953), Chatterjee (1981), Bruun, Par, and Norval (1975), Bailey (1935) and Gilmore (1991).

the evolutionary patterns identified in the literature are not applicable across them.[87] However, there are some definite trends.

First, the UN has been playing a prominent role in the development of such conventions in the latter half of the 20th century, although institutions such as the Organisation for Economic Cooperation and Development (**OECD**)[88] and the Council of Europe (**COE**) are also involved. The inter-war period saw enthusiasm for suppression conventions, with a number of conventions developed,[89] but since the 1970s the use of—and faith in[90]—such instruments has increased at a dramatic rate.

Second, these conventions have gone from relatively sparse documents, with only a handful of provisions, to quite the opposite.[91] This has not always translated into deep provisions, and many commitments could be said to be aspirational, rather than obligatory. Provisions often only prompt State Parties to consider certain improvements in their legal systems,[92] or in their cooperation with foreign law enforcement.[93] Requiring, for example, that States provide 'expeditious' mutual legal assistance provides little guidance as to how quick this assistance must be. There is no model response rate that States can look to, as it is dependent on a variety of factors, such as the LEA capacities of the requested State. The risk of reputational harm, even when response times stretch to over a year, is normally little. However, by and large, the demands

[87] See e.g. Andreas and Nadelmann (2006), 20-21, where the first two stages would not be applicable to cybercrime; in the first stage most societies are said to regard the activity as entirely legitimate, while in the second stage, the activity is redefined as a problem and an evil. Most of the crimes enumerated within the Cybercrime Convention were simply new ways of committing pre-existing offences, and were already prohibited in many counties.

[88] See e.g. the OECD Convention on Combating Bribery of Foreign Officials, (37 ILM 1, 1997).

[89] See e.g. the International Convention for the Suppression of Counterfeiting Currency (112 UNTS no. 2623, Geneva, 1929), (the **Counterfeiting Currency Convention**).

[90] Blum (2008), 324 describes 'universalists' as those who "believe that multilateral treaties … are both the cause and the effect of a transition from anachronistic notions of sovereignty and self-aggrandizement—still epitomized in bilateral, power-based pacts—to a more enlightened international society."

[91] Compare, for example, the Convention for the Suppression of Unlawful Seizure of Aircraft (860 UNTS no. 12325, The Hague, 1970), (the **Hijacking Convention**) with the Convention Against Corruption (2349 UNTS no. 42146, New York, 2003), (the **UNCAC**).

[92] See e.g. Article 20 UNTOC and Article 50 UNCAC which asks States to implement special investigative techniques, but only "to the extent permitted by the basic principles of its domestic legal system" and only "within its means."

[93] See e.g. Article 19 UNTOC and Article 49 UNCAC, which suggest that States should consider concluding arrangements for joint investigations.

placed on those that ratify these conventions have increased dramatically; as faith in the system grew, the depth of commitments grew correspondingly.

A third trend is that there is a definite "classic pattern"[94] to these conventions and many provisions repeat verbatim the texts of their predecessors.[95] This borrowing of, and building from, earlier models is partly explained by continuity in some of the personnel involved in the drafting of some conventions[96] and the use of models during negotiations.[97] But more obviously, it is a consequence of the success of previous provisions (or at least the avoidance of any significant problems emerging), which placates concerns about the implications of provisions, and negotiators can also take solace from the fact that their predecessors previously made such commitments, thus easing negotiations and expediting the ratification process. A final observation is that these conventions are overwhelmingly law enforcement oriented instruments. Clarke, speaking generally about many of the suppression conventions, states "[t]he treaties which have been discussed are for the most part 'law and order' rather than 'human rights' documents and concern for the rights of the accused is not in the forefront of any of them."[98]

To demonstrate these trends, it will be sufficient to consider the development of three significant issues found in most suppression conventions: jurisdiction, mutual legal assistance, and extradition.

3.4.1. Jurisdiction

In the early days of development of suppression conventions, drafters were reluctant to even mention criminal jurisdiction within the texts. This is demonstrated by Article 17 of the Counterfeiting Currency Convention 1929, which assures States that the "Convention shall not be interpreted as affecting that Party's attitude on the general question of criminal jurisdiction as a question of international law." Soon, however, it was realised that a natural

[94] Henrichs (1960), 1.
[95] See e.g. how the UNTOC built on the Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1582 UNTS no. 27627, Vienna, 1988), (the **Drugs Trafficking Convention**), and how the UNCAC built on the UNTOC.
[96] See Clark (1988), 86, and Andreas and Nadelmann (2006), 243.
[97] Nadelmann (1993), 346.
[98] Clark (1988), 86.

corollary of requiring a State to criminalise certain activities was to require that States establish territorial jurisdiction over such offences so as to permit prosecutions. It was unlikely to have been controversial even in the early years; every State expects to be able to prosecute acts committed within its territory, and for other States to be able to do likewise. The benefit of the latter is also that it prevents havens for the suppressed activity and all recent suppression conventions now make territorial jurisdiction,[99] and certain *sui generis* forms of territoriality (e.g. a vessel's flag State, and State of registration of aircrafts),[100] mandatory for ratifiers.

Requiring ratifying States to establish provisions concerning extraterritorial jurisdiction was more controversial. While prevalent in civil law countries, some, such as the UK, were traditionally reluctant to exercise anything other than territorial jurisdiction for most offences, and mandating that countries establish extraterritorial jurisdiction risked States distancing themselves from the instrument at hand. Therefore, with some exceptions,[101] extraterritorial jurisdiction is usually only suggested, with States preserving the right not to apply it. But there are a diversity of forms of extraterritorial jurisdiction found in the conventions: passive personality;[102] nationality;[103] habitual residence;[104] habitual residence when the person is stateless;[105] as well as more unorthodox

[99] See e.g. Article 5(1) Convention Against the Taking of Hostages (1316 UNTS no. 21931, New York, 1979), (the **Hostages Convention**), Article 4(1)(a)(i) Drugs Trafficking Convention, Article 3(1)(a) Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons (1035 UNTS no. 15410, New York, 1973) (the **Protected Persons Convention**), Article 6(1)(a) Convention for the Suppression of Terrorist Bombings Convention (2149 UNTS no. 37517 New York, 1997) (the **Terrorist Bombings Convention**), Article 15(1)(a) UNTOC and Article 42(1)(a) UNCAC.

[100] See e.g. Article 3(1)(a) 1973 Protected Persons Convention, Article 4(1)(a) Hijacking Convention, Article 5(1) Hostages Convention, Article 4(1)(a)(ii) Drugs Trafficking Convention, Article 6(1)(b) Terrorist Bombings Convention, Article 15(1)(b) UNTOC, and Article 42(1)(b) UNCAC.

[101] On nationality jurisdiction see e.g. Article 5(1)(b) Hostages Convention, Article 3(1)(a) 1973 Protected Persons Convention, Article 6(1)(c) Terrorist Bombings Convention and Article 6(1) Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (1678 UNTS no. 29004, Rome, 1988), (the **SUA Convention**).

[102] See e.g. Article 6(2) SUA Convention and Article 5(1)(d) Hostages Convention.

[103] See e.g. Article 6(2)(a) Terrorist Bombings Convention 1997, Article 42(2)(a) UNCAC, and Article 15(2)(a) UNTOC.

[104] See e.g. Article 4(1)(b)(i) Drugs Trafficking Convention.

[105] See e.g. Article 5(1)(b) Hostages Convention, Article 6(2)(c) Terrorist Bombings Convention, and Article 6(2)(a) SUA Convention.

grounds such as compelling a State to do or abstain from an act;[106] or where the offence is committed "against the State Party."[107]

Jurisdictional provisions concerning inchoate crimes, such as conspiracy and attempts, are a recent development. Clarke has long ago expressed concern about the elements of culpability in relation to offences such as conspiracy, which have "shown remarkable resiliency in finding [their] … way into many of the treaty formulations",[108] and calling for more thought to be given to such definitional issues in the criminalisation provisions. His call for definitional clarity in suppression conventions has not been heeded, and a striking subsequent development has been that these criminalisation provisions relating to inchoate crimes are now supplemented by jurisdictional provisions which prompt States to establish jurisdiction over extraterritorial inchoate acts (e.g. attempts or acts in furtherance of a conspiracy), if they are committed with a view to an offence within the jurisdiction.[109] The calculus for permitting such extraterritorial seizures of jurisdiction is explained by Boister:

> The suppression conventions provide vehicles for the reasonable extension of parties' jurisdiction with the agreement of other states, thus avoiding controversial unilateral assertions. By adopting a particular convention the parties make reciprocal grants of special competence on the jurisdictional principles listed in the conventions and in doing so waive their rights to object to the establishment of extraterritorial jurisdiction on the basis of these principles.[110]

Nevertheless, the costs of this approach are striking in some instances. For example, permitting extraterritorial jurisdiction on the grounds of habitual residence allows a country to prosecute a national of another country, even if the crime was committed in the latter. Another controversial provision is Article 4 of the Tokyo Convention,[111] which sets out the general rule that only the State of registration of an aircraft may interfere with it in flight in order to

---

[106] See Article 6(2)(d) Terrorist Bombings Convention and Article 6(2)(c) SUA Convention.
[107] Article 42(2)(d) UNCAC. In the EU context, see Article 12(2)(b) of the Directive on Attacks Against Information Systems (2013/40/EU, 12 August 2013), which envisages States establishing jurisdiction where the "offence is committed for the benefit of a legal person established in its territory."
[108] Clark (1988), 86.
[109] See e.g. Article 4(1)(b)(iii) Drug Trafficking Convention, Article 15(2)(c) UNTOC and Article 42(2)(c) UNCAC.
[110] Boister (2012), 137.
[111] Convention on Offences and Certain Other Acts Committed on Board Aircraft (704 UNTS no. 10106, Tokyo, 1963), (the **Tokyo Convention**).

exercise its criminal jurisdiction over an offence committed on board. It then, however, proceeds to provide an incredibly broad list of permissive extraterritorial grounds for such interferences, which essentially swallow up the general rule. [112]

The drafters of these conventions therefore embrace concurrent jurisdiction and the prospect of different countries attempting to exercise jurisdiction over a particular individual. As Ram notes, "[a]t every level, officials are confronted with the desire to avoid overlapping and potentially-inconsistent criminal and jurisdictional laws, while at the same time ensuring that there are no jurisdictional gaps for offenders to exploit." [113] The latter desire has overwhelming won the majority vote, and in most conventions provisions are even added which re-iterate that States may implement jurisdictional grounds other than those found in the convention, if they so desire.[114] This trend can also be seen within the EU. Klip, for example lambasts the EU's recent approaches to jurisdictional principles, observing that the "idea that additional extra-territorial jurisdiction for Member States will be conducive to enforcement prevails over the task provided for in Article 82 TFEU to prevent conflicts of jurisdiction."[115]

Many in the literature support this move towards extraterritoriality,[116] seeing it both as an inevitable[117] and desirable[118] response to globalised crime.[119] Even in the context of cybercrime where, as I will show,[120] there is often little need for

---

[112] Clark (1988), 55.
[113] Ram (2011), 10.
[114] See e.g. Article 5(3) Hostages Convention, Article 6(5) Terrorist Bombings Convention, Article 3(3) of the Tokyo Convention), Article 6(5) SUA Convention, Article 4(3) Drug Trafficking Convention, Article 15(6) UNTOC, and Article 42(6) UNCAC.
[115] Klip (2012), 199.
[116] One corrective is Parrish (2012), who challenges the trend because of its inefficiency and the rarity of prosecutions on extraterritorial grounds, the confusion caused from the resulting jurisdictional concurrency, and because it ultimately only provides "the illusion that serious steps are being taken to address transnational crime (often to mollify domestic constituencies), when in reality little is being done." Ibid, 290.
[117] See e.g. Buxbaum (2009), 668: "[t]he 'borderless' nature of some activities, the near-global nature of others—all of this seems to demand regulatory solutions freed from territorial underpinnings."
[118] See e.g. Gable (2010), 118: "… the most feasible way to deter cyberterrorism is through the international law principle of universal jurisdiction." See also Kramer (1991), 184: "… the world in which a presumption against extraterritoriality made sense is gone."
[119] Even the UK's aversion to extraterritorial jurisdiction is seemingly changing. See e.g. s.12 of the Bribery Act 2010.
[120] See chapters five and seven.

reliance on extraterritorial jurisdiction due to the breadth of the concept of territoriality, it is being mandated.[121]

3.4.2. Mutual Legal Assistance

The second issue I have highlighted, in order to demonstrate the trends of suppression conventions, is MLA. Including MLA provisions in these conventions is a relatively recent phenomenon,[122] but the breadth, detail, and depth of commitments have increased dramatically, particularly since the UN's Drug Trafficking Convention 1988.[123] These suppression convention provisions are exclusively LEA-oriented measures, with suspects and defendants remaining the "objects of MLA and cannot derive from the MLA scheme rights to gather evidence."[124] The trend has been to insert sections that seek to ensure the widest possible measure of MLA,[125] as quickly as possible,[126] and to remove the traditional barriers to its exercise.[127] Optional grounds for refusal certainly remain, often tied to notions of sovereignty,[128] however, other provisions are frequently inserted to edge parties towards provision of MLA, by requiring reasons for refusal,[129] or consultation so as to determine whether some assistance can be provided that would not jeopardise local proceedings.[130] The conventions have also sought to embrace less formal methods of cooperation, suggesting voluntary provision of information to other countries,[131] and providing for general obligations to cooperate with counterparts in conducting enquiries, and establishing channels of

[121] See Article 12(1)(b) Directive on Attacks Against Information Systems (2013/40/EU, 12 August 2013).
[122] See generally Vervaele (2014) and Joutsen (2014).
[123] See Vervaele (2014), 125, for a comparison between the MLA provisions in the Drugs Trafficking Convention and the UNTOC.
[124] Vervaele (2014), 135.
[125] See e.g. Article 7(1) Drug Trafficking Convention 1988, Article 46(1)&(2) UNCAC and Article 18(1)&(2) UNTOC.
[126] Article 46(24) UNCAC and Article 18(24) UNTOC.
[127] See e.g. provisions which obligate States not to refuse MLA on the ground of bank secrecy: Article 18(8) UNTOC, Article 46(8) UNCAC and Article 7(5) Drug Trafficking Convention. On alleviating dual criminality requirements, see Article 18(9) UNTOC and Article 43(2) UNCAC.
[128] Vervaele (2014), 136. See provisions relating to prejudicing the security or *ordre public* of the requesting country: Article 46(21)(b) UNCAC and Article 7(15)(b) Drug Trafficking Convention. See also provisions relating to prejudicing ongoing domestic investigations or prosecutions: Article 7(17) Drug Trafficking Convention and Article 46(25) UNCAC.
[129] See e.g. Article 18(23) UNTOC and Article 46(23) UNCAC.
[130] Article 7(17) Drug Trafficking Convention.
[131] Article 18(4) UNTOC, Article 46(4) UNCAC and Article 14 SUA Convention.

communication for the secure and rapid exchange of information.[132] As we will see in the next chapter, the Cybercrime Convention has been even more innovative in this regard.

In practice, MLA does not operate anywhere nearly as quickly and efficiently as these provisions might suggest they would,[133] due to basic factors such as bureaucratic inefficiency, capacity, workloads, or sheer reluctance due to political differences. However, in the context of cybercrime, this is not proving insurmountable for many countries, as the next chapter demonstrates.

3.4.3. Extradition

The aforementioned trends of suppression conventions can also be discerned from looking at how extradition provisions are being inserted and are developing. Extradition is another process that was absent from the earlier conventions, but soon became a regular stable-mate in all of them.[134] Typically the conventions will deem the suppressed offences to be extraditable under extradition treaties existing between Parties,[135] will enable the suppression convention itself to serve as an extradition treaty if one party requires such for extraditions to proceed,[136] or if parties do not require an extradition treaty, it requires them to consider the suppressed offences as extraditable.[137] Therefore, extradition provisions in conventions normally focus only on ways to facilitate

---

[132] See e.g. Article 9(1) Drug Trafficking Convention.

[133] The UNODC Cybercrime Study (2013), 206 (see below section 4.2.2.3) indicated that the average response time for MLA in cybercrime cases is 150 days. However, it is not clear how reliable or representative this data is, since only 16 countries responded to this particular question, and the question did not specify the types of response to which it was referring e.g. substantive resolution versus acknowledgment of receipt. Practitioners have confirmed to me that responses are generally in the order of months, rather than days, and Kent (2014), para. 20, notes that UK LEA experience is such that "requests for communications data through MLA can take between 8 and 13 months."

[134] On extradition provisions in suppression conventions, see Harrington (2014). For a broader analysis of international extradition laws see Bassiouni (2014).

[135] See Article 10 Counterfeiting Currency Convention, Article 10(1) Hostages Convention, Article 8(1) Protected Persons Convention, Article 8(1) Hijacking Convention, Article 11(1) SUA Convention, Article 6(2) Drugs Trafficking Convention, Article 16(3) UNTOC and Article 44(4) UNCAC.

[136] See Article 8(2) Hijacking Convention, Article 8(2), Protected Persons Convention, Article 10(2) Hostages Convention, Article 11(2) SUA Convention, Article 6(3) Drugs Trafficking Convention, Article 16(4) UNTOC and Article 44(5) UNCAC.

[137] See Article 10 Counterfeiting Currency Convention, Article 8(3) Hijacking Convention, Article 8(3) 1973 Protected Persons Convention, Article 10(3) Hostages Convention, Article 6(4) Drugs Trafficking Convention, Article 16(6) UNTOC and Article 44(7) UNCAC.

the process, rarely considering safeguards for the accused,[138] or if they do, try to prompt States into interpreting these safeguards broadly.[139] Provisions have become common which ask parties to simplify and expedite extradition procedures, lower evidential thresholds,[140] and remove barriers to extradition.[141]

The conventions now also invariably contain an obligation to prosecute or extradite *(aut dedere aut judicare)*,[142] with a variety of formulations emerging[143] but commonly based on Article 7 of the Hijacking Convention (known as the "Hague formulae")[144] which stipulates that "[t]he Contracting State in the territory of which the alleged offender is found shall, if it does not extradite him, be obliged without exception whatsoever and whether or not the offence was committed in its territory, to submit the case to its competent authorities for the purpose of prosecution."[145] This deep provision clearly envisages prosecutions even where the prosecuting State cannot point to jurisdiction under any of the traditional heads, and the conventions therefore supplemented such obligations with requirements to establish jurisdiction to cater for such prosecutions.[146] On other occasions, the conventions have even

---

[138] One exception here is the non-discrimination clause, found in Article 9(1) Hostages Convention, Article 6(6) Drugs Trafficking Convention and Article 44(15) UNCAC.

[139] See e.g. Article 43(2) UNCAC which deems dual criminality requirements as being fulfilled, irrespective of legal classification, provided the underlying conduct constitutes an offence in both countries. This approach to dual criminality is common in the MLA provisions of suppression conventions, and now in UK extradition law, as discussed in chapter seven.

[140] See Article 6(7) Drugs Trafficking Convention, Article 16(8) UNTOC and Article 44(9) UNCAC.

[141] See e.g. Article 16(15) UNTOC and Article 44(16) UNCAC, which prevent parties from refusing extradition on the ground that the offence involves fiscal matters. Harrington (2014), 158 also notes, in the context of political offence exceptions, that a number of "exceptions to the exception" have developed.

[142] The Latin term is normally traced to Grotius's phrase '*aut dedere aut punire'* (extradite or punish), the former being a modern equivalent which is less presumptive of guilt. See Grotius (1925). However, Mitchell (2009), chapter 1, para. 58 observes how the principle has been traced back to Bodin and Baldus in the 14th century.

[143] See the Final Report of the International Law Commission, 'The Obligation to Extradite or Prosecute (aut dedere aut judicare)', *Yearbook of the International Law Commission* (2014), vol. II Part two, para. 12, (the **ILC Report 2014**).

[144] The ILC notes that "[o]f the conventions drafted on or after 1970, approximately three-quarters follow the "Hague formula." See ILC Report 2014, para. 13.

[145] As the ILC note, this "does not unequivocally resolve the question of whether the obligation to prosecute arises *ipso facto* or only once a request for extradition is submitted and not granted." (ILC Report 2014, para. 40. Plachta (1999), 133 has argued that there should not be a hierarchy between an obligation to extradite or prosecute, and decisions should be based on "mutual consultations between the appropriate authorities." See also Olson (2011), 327 and Abelson (2009). As shall be seen in chapter six, however, there is little to guide such consultations.

[146] See Article 4(2) Hijacking Convention. This provision was a late amendment, justified on the following grounds: "The reason behind [this] proposal was that Article 7, which obliged

created what Clarke has called "territorial fiction[s]."[147] The need for this fiction arose because many bilateral extradition treaties allowed extradition to proceed only if the requesting State could point to offences committed within its 'territory' or 'jurisdiction.' In order to overcome such a restriction and facilitate extradition on extraterritorial grounds, some conventions created a fiction that treated acts committed outside of the territories of the requested or requesting Parties as having been committed within them.[148] As we will see in the context of cybercrime, there is little need for the creation of such fictions; territorial jurisdiction is frequently there for any State that wants it.

3.5 Harmonisation through the Cybercrime Convention

The seeds to the Council of Europe's 'Convention on Cybercrime' were laid many years before it was opened for signature in November 2001. The OECD appointed an expert committee in the early 1980s which published a report recognising the "desirability for international cooperation" and listing five categories of offences which could be adopted in domestic penal legislation.[149]

States that did not concede extradition to submit the case to their competent authorities for their decision whether to prosecute, would be a dead letter provision if States did not have jurisdiction under Article 4, paragraphs 1 or 2." International Civil Aviation Organization, *International Conference of Air Law, The Hague,* December 1970, Volume I: Minutes (Doc. 8979-LC/165-1), Spain (8th meeting of the Commission of the Whole, para. 17 p.75). The ILC neglected the role of 'vicarious' or 'representational' jurisdiction in some of these jurisdictional provisions in suppression conventions, stating broadly that they "necessarily reflect an exercise of universal jurisdiction": ILC Report (2014), para. 18. Vicarious or representational jurisdiction is "not widely used by States" (Ryngaert (2008), 102) and its parameters are neither settled in international law, but it is generally understood to allow extraterritorial custodial States to prosecute where there are legal obstacles with the extradition and double criminality is met (see e.g. Ryngaert (2008), 102, Chehtman (2010), 76-7, Blakesley and Lagodny (1991), 36 and Meyer (1990)). The ILC failed to distinguish between the two forms of jurisdiction. As Ryngaert (2008), 103, observes: "States, when exercising representational jurisdiction, protect the interests of the territorial State, whereas, when exercising universal jurisdiction, they (supposedly) protect the interests of the international community." Many *aut dedere aut judicare* provisions in conventions which adopt the Hague formula are suggestive of any prosecution being a representative prosecution for the requesting State, as they refer to decisions regarding prosecution having to be made through consultation or discussion with the State which requested extradition, or information being communicated to that State regarding the outcome of the decision of whether to prosecute or not (including in the Cybercrime Convention, Article 24(6)). The corollary jurisdiction involved in the 'Hague formulae' has therefore been referred to as "representative universal jurisdiction" (Kreß (2006), 567) or "co-operative limited universality" (Reydams (2003), 28).

[147] Clark (1988), 59.

[148] See e.g. Article 11(4) SUA Convention, Article 8(4) Hijacking Convention and Article 10(4) Hostages Convention. Another form of this territorial fiction, not discussed by Clarke, is Article 9 Counterfeiting Currency Convention.

[149] OECD, 'Computer-Related Criminality: Analysis of Legal Policy in the OECD Area', Report DSTI-ICCP84.22 (1986), discussed in Walden (2004), 322, and Schjolberg (2008).

Shortly before the publication of this report, the COE had itself appointed an expert committee, which also published a report, and a non-binding Council of Minister's Recommendation, containing a list of eight computer-related offences (and an additional four which were optional, due to lack of consensus) which governments were urged to adopt.[150] This was supplemented in 1995 when the COE agreed another Recommendation concerning the procedural issues arising from computer crime.[151] A final important seed to the Convention was the work of the G8, who adopted a number of principles towards combatting 'high-tech crime' in the late 1990s, including principles relating to preservation of data stored in a computer system, expedited MLA, and transborder access to stored data not requiring legal assistance.[152]

Therefore, much of the groundwork had been done when the 'Committee of Experts on Crime in Cyber-space' (**PC-CY**) began working on a draft convention, a task it was given in February 1997.[153] The work of the PC-CY was shrouded in controversy at the time and little is known even about the make-up of the group, except that Professor Henrik Kaspersen was intimately involved, chairing the Committee of Experts.[154] As Banisar and Hosein noted,

---

[150] Report by the European Committee on Crime Problems 'Computer-Related Crime' and Recommendation No. R(89) 9, (Strasbourg, 1990).
[151] Recommendation No. R(95)13.
[152] Ministerial Conference of the G8 Countries on Combatting Transnational Organized Crime, 'Principles on Transborder Access to Stored Computer Data', (Moscow, 19-20 October 1999). See also Meeting of Justice and Interior Ministers of the Eight, 'Principles and Action Plan to Combat High-Tec Crime', Communiqué (9-10 December 1997).
[153] Committee of Ministers, Decision no. CM/Del/Dec(97) 583 (February 4th 1997). The European Committee on Crime Problems had also, the previous year, set up a committee of experts tasked with examining a range of cybercrime issues, the work of which fed into the PC-CY. A more thorough account of the background to these groups is contained in the Explanatory Report to the Cybercrime Convention, paras. 7-15.
[154] Kaspersen (2006), 9. Schjolberg (2008), 2 describes him as the "father" of the convention. The author has also learned (following an intervention at an Octopus Conference on Cooperation against Cybercrime, 4-6 December 2013) that Betty Shave was one of the US representatives involved in the drafting process. The text of the Convention suggests that the US had a powerful role in shaping the normative content of this document with many provisions closely resembling procedural powers found in US law (see, for example, my discussion of the wording of Article 32(b) and provisions of the Stored Communications Act at 4.2.2 and 4.2.2.3 below). The extent of US involvement is likely to have been due to the fact that they are the global policing hegemon, as discussed in chapter one, with significant experience in investigating and prosecuting cybercrime, and had relatively comprehensive laws covering investigative powers and the crimes under discussion, at the time of the negotiations. Representatives from Canada, Japan, and South Africa were also involved.

"[t]his process has been exceedingly secretive and has not benefited from any input except from selected law enforcement officials for several years."[155]

Eventually, a draft of the Convention was published in April 2000, followed by a number of amended versions, but very few of these amendments responded to industry concerns, or those from civil society groups.[156] In fact, one of the only new provisions inserted after the publication of the October 2nd 2000 draft,[157] was Article 15—Conditions and Safeguards. But this is one of the most shallow and superfluous provisions in the entire convention. Article 15(1) requires States to ensure that their implementation provides "adequate protection of human rights", including rights which arise under instruments such as the European Convention on Human Rights (**ECHR**), and the International Covenant on Civil and Political Rights. States that are a party to these instruments are, however, already bound by them in their domestic legislative activities. Similarly, Article 15(2) requires Parties to consider appropriate levels of oversight for the exercise of procedures and powers under the Convention, but this would not prevent countries such as the UK continuing to allow police access to communications data under the Regulation of Investigatory Powers Act 2000 (**RIPA**), pursuant to an internally authorised police request. Article 15(3), in a similar vein, requires States to, *inter alia*, consider the rights of third parties, but only "[t]o the extent that it is consistent with the public interest." Article 15, therefore, seems only to serve one of the functions of 'symbolic legislation': that of reassuring the public.[158]

Nevertheless, the Convention was opened for signature on the 23rd November 2001, and entered into force on the 1st July 2004. It is currently signed by all COE Member States except Russia and San Marino, and ratified by forty-four

---

[155] Banisar and Hosein (2000), 5.
[156] Ibid. See the letter sent to the COE by a number of interested parties: 'Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime Version 24.2' (December 12th 2000). Available at: http://gilc.org/privacy/coe-letter-1200.html (Accessed 20/12/2014). See also Article 29 Data Protection Working Party, 'Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-crime', 5001/01/EN/Final WP 41.
[157] Draft Convention on Cybercrime (Draft No. 22 REV). The only other entirely new provision (not including chapter IV Final Provisions), found in the final convention was Article 26 on spontaneous information provision, which was certainly not one of the demands of the aforementioned civil society groups.
[158] Marion (2010), 702.

countries, including six non-members of the COE (Australia, Dominican Republic, Japan, Mauritius, Panama, and the US).[159]

The Convention is split into four chapters: (1) Use of Terms (2) Measures to be taken at domestic level – substantive and procedural law (3) International Co-operation and (4) Final Clause. An analysis of its provisions very much reveals that it followed the orthodox approach: harmonise criminal laws and procedures, improve international cooperation, and innovate where possible to improve these aims. Section 1 of Chapter II outlines nine different types of cybercrimes, as well as ancillary liability[160] and sanctions,[161] which must be transposed into domestic law—a large number that is very much in keeping with more recent suppression conventions. One set of crimes over which there was insufficient 'moral consensus', was in relation to the distribution of racist propaganda through computer systems. Although discussed by the PC-CY, it was eventually excised from the Convention,[162] and placed in an Additional Protocol.[163] This was done so as not to jeopardise agreement on the remainder of the Convention, and even in the Protocol, reservation provisions emasculate most of the criminalisation obligations.[164] These crimes, as well as those found in the Convention itself, will be analysed in detail from a domestic (UK) jurisdictional perspective in chapter five.

Section 2 of Chapter II deals with elements of procedural law that were recognised as being required for many cybercrime investigations, as well as other criminal investigations where evidence pertaining to an offence may be stored in electronic form.[165] These concern production orders, search and

[159] Status of 20 December 2014. Article 37 of the Convention allows the Committee of Ministers to invite any State to accede to the Convention.
[160] Article 11: attempt and aiding and abetting.
[161] Article 13 is, however, a shallow provision which simply requires States to ensure "effective, proportionate and dissuasive sanctions."
[162] Para. 35 of the Explanatory Report to the Cybercrime Convention.
[163] Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems (CETS no. 189, 2003). Twenty-two countries have ratified the Protocol.
[164] See e.g. Articles 3(3), 5(2)(b) and 6(2)(b).
[165] Article 14(2)(b) envisages that the powers in the Convention will be utilised for investigations relating to any criminal offences committed through computer systems—even beyond the cybercrimes which must be suppressed in the Convention—while Article 14(2(c) states they should apply to the collection of evidence in relation to any other criminal offences as well.

seizure of stored computer data, collection of traffic data,[166] and the interception of content data. As per the trend of suppression conventions, innovations were made on previous conventions. Article 16, for example, requires Parties to adopt legislation to enable the expeditious preservation of specified computer data, including traffic data, for as long as is necessary, up to ninety days.[167] From the latest available study, only fourteen countries that are Party to the Convention have implemented specific legislation providing for such a power,[168] and preservation is rarely utilised in practice in most State Parties, with the exception of the US, where thousands of preservation orders are issued annually.[169] This may be due to a preference for seizing the data directly through production orders,[170] but also because within the EU, data retention obligations[171] have previously been placed on certain service providers, in relation to certain categories of data, which may often negate the need for preservation.

Section 3 of Chapter II addresses the issue of jurisdiction and this is where the drafters were at their most conservative and unoriginal. State Parties must establish jurisdiction over offences committed in its territory, on its ships or aircrafts or by one of its nationals.[172] Only territorial jurisdiction, however, is mandatory, as States can enter reservations in relation to the other grounds.[173] As Hayashi notes, this follows the "established pattern of jurisdiction in

---

[166] Within the UK, this is a powerful investigative tool which does not require judicial authorisation; Part 1, chapter II of the Regulation of Investigatory Powers Act 2000 (**RIPA**) allows access to communications data within seconds via the secure Criminal Justice Extranet (**CJX**) and an internally authorised LEA request. For an illustration of how the system works, see Hoskins (2012).
[167] Article 16(2).
[168] 'Assessment Report: Implementation of the Preservation Provisions of the Budapest Convention on Cybercrime' (T-CY, 8th Plenary, 5-6 December 2012), 7, (**Assessment Report**).
[169] Ibid, 10.
[170] Ibid, 7.
[171] The Data Retention Directive (2006/24/EC, 15 March 2006) required Member States to place providers of publicly available electronic communications networks and services, within their territories, under an obligation to retain certain communications data, for any period between six months and two years. This was, however, recently declared invalid by the Court of Justice of the European Union (**CJEU**) for interfering with various rights in the Charter of Fundamental Rights of the European Union. See *Digital Rights Ireland and Landesregierung* (Joined Cases C-594/12 and 293/12, of 8 April 2014). The UK has introduced emergency legislation in the form of the Data Retention and Investigatory Powers Act 2014, to ensure that operators can continue to be placed under retention requirements.
[172] Article 22(1).
[173] Article 22(2).

treaties prior to the information revolution"[174] and "[n]othing in the rules of jurisdiction suggests that cyber-crimes are more transnational or more challenging than other types of crimes."[175]

The patterns of suppression conventions are also very much to be seen in Chapter III, which deals with international cooperation. For example, the aforementioned hallmarks of extradition provisions in these conventions are found verbatim in Article 24, while the MLA articles emphasise speed,[176] breadth in provision,[177] and the alleviation of known barriers.[178] Furthermore, nearly all of the procedural mechanisms from Chapter II, Section 2, have corresponding provisions in Chapter III to enable international cooperation, with various innovations to fit this particular criminality. Article 29 enables inter-State requests for obtaining the expeditious preservation of data. There are limited grounds for refusal,[179] a prohibition on imposing dual criminality as a condition for refusal,[180] and further obligations on the requested State when it discovers certain information in the course of the execution of a request.[181] Provision is also made for the accessing of such data,[182] and for MLA in relation to the real-time collection of traffic data,[183] and interception of content data.[184] I will analyse further particular procedural innovations found in the Convention in the next chapter.

---

[174] Hayashi (2007), 79.
[175] Ibid, 78.
[176] Article 25(3).
[177] Article 25(1).
[178] See e.g. Article 25(5), which requires that Parties do not adopt a 'list' approach to dual criminality, but will look to underlying conduct.
[179] Article 29(5).
[180] Article 29(3), though see Article 29(4).
[181] When acting in compliance with Article 29 and a requested Party "discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted" (Article 30). This is a vague obligation, and it will be difficult to ascertain compliance, but further evidences the Convention's attempted regularisation of LEA networking and cooperation. No Party to the Convention has enacted specific legislation on Article 30: see Assessment Report 2012, *supra* note 168.
[182] Article 31.
[183] Article 33.
[184] Article 34.

3.6 Conclusion

The common assumption is that transnational crime is resulting in the loss of State control,[185] and in no sphere is this truer than in the realm of cybercrime. As Andreas notes, "for centuries, law enforcement officials have bemoaned the crime-enabling effects of new technologies, and have used this as a rationale to further expand their policing reach."[186] A suppression convention was the natural reaction by States. Regardless of the ultimate success of previous initiatives,[187] the suppression convention is seen as the ultimate panacea and, as has been demonstrated, a definite pattern has developed across these conventions. These patterns include the homogenisation of criminal and procedural laws, the enablement of inter-State cooperation, and the maintenance of jurisdictional breadth so as to prevent safe havens of criminality. It is assumed with this final development that when States agree a suppression convention, jurisdictional conflict dissipates because local enforcement indirectly benefits foreign sovereigns[188] and because the priority shifts to preventing impunity.[189]

I contend that this can be characterised as an example of what Brenner has coined "the fallacy of inevitability (or, business as usual): the tendency to assume that reified, institutionalized patterns of behaviour are necessary and, indeed, inevitable."[190] The assumption in the Convention is that cybercrime is just like any other crime—suppress the activity, extend the reach of law enforcement, and ensure all States can assert jurisdiction, and it will be business as usual. There is no attempt to envisage how cybercrime may create problems of concurrent jurisdiction on a new scale, or to develop new methodologies to cope with them. In fact, the only attempt being made to amend the Convention is to further expand the transnational access to data for

---

[185] As Shelley (2011), 3 notes "the control of crime is state-based, whereas nonstate actors such as criminals and terrorists operate transnationally, exploiting the loopholes within the state-based systems."
[186] Andreas (2011), 414. See also Deflam (2002)
[187] While States have enjoyed relative success in suppressing activities such as counterfeiting currency, due to its ability to remain a technological step ahead of counterfeiters, their success in areas such drug control are much more questionable.
[188] Kohl (2007), 220.
[189] Hayashi (2007), 66.
[190] Brenner (2013), 225. Brenner uses the term to discuss internal US cybercrime policies, and the limits of bureaucratic control, but it is particularly apt in this context as well.

law enforcement, which will be discussed at some length in the next chapter. The current suggested changes very much continue the trend of being exclusively law enforcement oriented measures,[191] and are blind to potential consequences for jurisdictional concurrency.

Within the context of the EU, however, Spencer draws a connection between EU instruments which require Member States to adopt forms of extraterritorial jurisdiction for criminal offences, mutual recognition, and choice of forum.[192] The connection is that the former two operate together to extend the number of countries that can investigate transnational crime; extraterritorial jurisdiction will ensure a State is not stymied in prosecution by territorial jurisdictional limitations, while mutual recognition instruments provide the tools for gaining access to both suspects, as well as evidence. He concludes that:

> It follows that these three things—mutual recognition, extra-territorial jurisdiction and choice of forum—are indeed connected. And from this it further follows that an intelligent discussion about choice of forum should take the other two corners of the triangle into account.[193]

The following chapters take on this challenge, but I also, more ambitiously, attempt to look at the bigger triangles that are of relevance to choice of forum in the context of cybercrime. Beyond the EU, harmonisation initiatives are strengthening,[194] furthering law enforcement access to information, and facilitating a broadening of territorial (as well as extraterritorial) jurisdiction; the triangulation of these elements and their impact on choice of forum, has garnered insufficient attention in the literature, particularly in the context of cybercrime, and is sorely in need of explication and appreciation.

---

[191] One difference from the initial drafting of the Convention, however, is the input which the T-CY has received from civil society.
[192] Spencer (2013), 72.
[193] Ibid.
[194] As of 2013, 82 countries have signed and/or ratified a binding cybercrime instrument: The Cybercrime Convention, the League of Arab States Convention on Combating Information technology Offences, the Commonwealth of Independent States Agreement on Cooperation in Combating Offences related to Computer Information, or the Shanghai Cooperation Organization Agreement in the Field of International Information Security. See UNODC Cybercrime Study (2013) Executive Summary, pg xix, which is discussed in more detail in the next chapter.

Chapter 4: Cybercrime Investigations

> "We don't need to go to a foreign country to get the records. The provider is right here."[1]

> "The Convention gives us a new tool to address the scourge of crime as a global problem. With enhanced international cooperation, we can have a real impact on the ability of international criminals to operate successfully."[2]

4.1 Introduction

It is trite to say that cybercrime investigations can be labyrinthine in nature. Any investigation could involve numerous service providers, including hosting providers, domain name registrars, payment providers, and webmasters, and criminals can switch providers in a matter of minutes, providing each with false registration information, thus hampering tracing.[3] Cybercriminals can also utilise virtual currencies like Bitcoin and anonymising software like TOR, in order to mask their identities, and even if IP addresses are available, these may relate to innocent users, whose compromised computer forms part of a botnet, or the relevant access provider may be unable to associate the IP address with any particular individual as it failed to maintain such records. Moreover, evidence in relation to the particular crime may be scattered across the world, as organised cybercriminals employ "strategies of displacement."[4] Criminal groups can operate loosely and informally fragmenting their activities across numerous territories with each performing discrete aspects of the larger criminal operation. A single investigation could involve hundreds of individuals in as many countries. When combined with the traditional territorial limits of enforcement jurisdiction, basic obstacles to cross-border

[1] US Attorney Serrin Turner. Available at: http://www.bloomberg.com/news/2014-07-31/microsoft-fails-to-block-u-s-warrant-for-ireland-e-mail.html (Accessed 20/12/2014).
[2] Secretary-General Kofi Annan, foreword to the United Nations Convention against Transnational Organized Crime and the Protocols Thereto (New York, United Nations, 2004).
[3] See O'Floinn (2011). Work is ongoing in ICANN to improve the validity of domain name registration information. See e.g. the work of the Generic Names Supporting Organization (GNSO) working group on "Privacy and Proxy Services Accreditation Issues."
[4] Sansom (2009). For discussion of some of the evidential issues that can arise at trial in cybercrime prosecutions, see O'Floinn and Ormerod (2012).

police cooperation such as language barriers,[5] and the snail-like pace of MLA, the challenges are clearly formidable.

While there is much truth in the claim that the combined forces of globalisation and the Internet are empowering cybercriminals to transcend and circumvent traditional State borders and control, it must also be realised "that the same networked technologies that empower criminals also provide a range of highly effective policing tools."[6] It has never been easier for police networks to operate so fluidly and so quickly either, but this "growing global reach of law enforcers" has been "far less noticed and even less understood",[7] and this is particularly true in cybercrime enforcement. Even the most sophisticated of cybercriminals, utilising and operating sites on the 'dark web',[8] can be unearthed with perseverance, international cooperation, and technological know-how.[9] Moreover, while many cybercriminals are technically-able actors, many clearly aren't.[10]

This chapter has a dual purpose. First, it seeks to elucidate the growing global reach of LEAs in cybercrime investigations. Second, it demonstrates my claim in chapter three that suppression conventions are almost exclusively law enforcement oriented instruments, which facilitate considerable inroads into the territorial limitations of enforcement jurisdiction. In fact, we will see that the concept of territoriality in this context is being completely transformed, and the Convention has no small part in this.

---

[5] See e.g. Hewitt and Holmes (2002), paper delivered at the Kent Criminal Justice Centre, discussed in Block (2012), 93.
[6] Wall (2007(a)), 201.
[7] Andreas and Nadelmann (2006), 223.
[8] This is only accessible through the TOR network. For more information on the 'Dark Web', see Bartlett (2014).
[9] This has been the case with the arrests of Ross Ulbricht, who has been charged with creating the online marketplace 'Silk Road', and Blake Benthall, who is being prosecuted for running its successor site. For further details of how these individuals were found, see *US v Blake Benthall* (New York Complaint, 14 MAG 2427, 29 October 2014), [38-47] and the prosecution submissions in the Ulbricht case: *US v Ulbricht*, Declaration of Christopher Tarbell (US District Court of New York, S1 14 Cr. 68, September 5 2014) and *US v Ulbricht*, Memorandum of Law in Opposition to Defendant's Motion to Suppress Evidence, Obtain Discovery and a Bill of Particulars (US District Court of New York, S1 14 Cr. 68, September 5 2014).
[10] This is well illustrated by the thousands of individuals that were identified attempting to coerce a computer-generated child to perform sexual acts over webcam. See http://www.bbc.co.uk/news/uk-24818769 (Accessed 20/12/2014). This operation was arranged by a private Dutch children's charity called Terre des Hommes. The dangers of such private investigatory practices (including entrapment), are addressed in O'Floinn and Ormerod (2011).

I begin with an analysis of some of the domestic procedural powers which must be implemented by State Parties to the Convention which, as will be shown, can be powerful tools regardless of where operators or data is located. The subsequent section considers discussions in the Council of Europe to further expand the transnational access to data by LEAs. Finally, I address the Convention's role in further entrenching, and fostering, the role of TGNs in this context.

4.2 Extending the Scope of Domestic Procedural Powers

As discussed in the previous chapter, one of the primary mechanisms for achieving the aims of a suppression convention is to require States to implement the procedural powers necessary for investigations concerning the offence(s) contained in the Convention. Domestic use of these powers to suppress domestic activity indirectly assists foreign States suffering from the transnational criminality, and it also facilitates cooperation in the form of MLA measures. Chapter II, section 2 of the Convention contains a range of mechanisms to this end, and the following focuses on some of these procedural provisions, notably production orders against domestic and foreign service providers and search and seizure measures, and how these can be used by cybercrime (and other)[11] investigators.

4.2.1. Domestic Production Orders

Article 18 of the Convention requires Parties to implement a production order, of which there are two forms mentioned: the first requires "a person in its territory to submit specified computer data in that person's *possession or control*…"[12] (the **person-in-territory production order**); the second requires "a service provider *offering its services in the territory* of the Party to submit subscriber information relating to such services in that service provider's

[11] Article 14(2)(c) provides that Parties shall apply the powers and procedures discussed below in relation to "the collection of evidence in electronic form of a criminal offence."
[12] Article 18(1)(a).

possession or control"[13] (the **service-in-territory production order**), and could relate even to foreign service providers (this will be discussed below).[14]

The potential scope of the person-in-territory production order has been demonstrated by the recent *Microsoft Warrant* case.[15] Here US authorities served a production order[16] on Microsoft in the US to obtain data, including the contents of emails, relating to one of its customers. The contents of the emails were stored on a server located in Dublin.[17] Microsoft argued, *inter alia,* that a warrant under section 2703(a) of the Stored Communications Act[18] (**SCA**) was to be distinguished from the operation of subpoenas, which have previously been used to compel production of business records stored extraterritorially;[19] a warrant, it argued, could not extend to the search and seizure of property outside of the US, and would require MLA.

This was not how Francis J. understood either the procedural power, or its operation. He found that "the order is a hybrid: part search warrant and part subpoena,"[20] as government agents did not enter Microsoft's premises to search its servers, and that this unique structure meant that the "SCA does not implicate principles of extraterritoriality."[21] The obligation on Microsoft was only "to act within the United States"[22] and the search occurred only when the information was "reviewed in the United States."[23] Congress was said to have "anticipated that ISPs located in the United States would be obligated to

---

[13] Article 18(1)(b).
[14] See section 4.2.2.
[15] *re Warrant to Search a Certain E-mail Account Controlled and maintained by Microsoft Corp*., F. Supp. 2d (SDNY 25 April 2014) (**the *Microsoft Warrant* case**).
[16] I deal with this as a production order under Article 18 of the Convention, rather than a search and seizure order under Article 19 of the Convention, as the latter (discussed below in section 4.2.3) is clearly intended to only apply to computer systems within the searching country's territory.
[17] This also suggests that the individual was based outside of the US, as Microsoft attempted to assign data centers near to where the user is located to prevent "network latency." *Microsoft Warrant* case, *supra* note 15, [2].
[18] 18 U.S.C. Chapter 121 § 2701-2712.
[19] In *Tiffany v Andrew* 276 FRD 143, 147-8 (SDNY 2011) it was said "[i]f the party subpoenaed has the practical ability to obtain the documents, the actual physical location of the documents – even if overseas – is immaterial."
[20] *Microsoft Warrant* case, *supra* note 15, 12.
[21] Ibid.
[22] Ibid, 22.
[23] Ibid, 14. The court drew on Kerr to this end, neglecting the fact that he refined his view in subsequent work, where he argued that copying data does constitute a search under the fourth amendment: Kerr (2010), 711-2.

respond to a warrant"[24] in this way, and the nationality principle was also drawn upon in order to support "the legal requirement that an entity subject to jurisdiction in the United States, like Microsoft, may be required to obtain evidence from abroad."[25] Finally, Francis J. considered the alternative available to LEAs (obtaining the information through MLA) and this was found to be impractical, as MLA remains "slow and laborious",[26] with countries "generally retain[ing] the discretion to decline,"[27] and it is unavailable where a treaty is not in place.[28]

Numerous aspects of the decision are highly questionable. First, reliance on nationality jurisdiction for criminal prosecutions against individuals does not logically entail production obligations against a corporation, relating to extraterritoriality-stored data. Second, the contention that Congress had intended section 2703(a) of the SCA to apply in this way was not convincingly demonstrated; as Kerr argues, the SCA was simply "not written with the territoriality problem in mind"[29] as it was drafted at a time where users, providers and communication over computer networks were mostly in the US.[30] Third, as Microsoft argued in its appeal brief, the government's argument that customer emails constituted Microsoft's business records creates a disjunction between the operation of production powers in the online and 'physical' world.[31] Fourth, it is illusory to say that Microsoft was only acting within the US, and that the search only occurred there, as servers in Ireland had to be accessed to copy and retrieve the data. Indeed the US government itself previously made a point of distinguishing between the place where the data is located, and the place where the search is conducted from, in order to preserve

[24] *Microsoft Warrant* Case, *supra* note 15, 18.
[25] Ibid, 22.
[26] Ibid, 19, citing Kerr (2014), 409.
[27] Ibid.
[28] Ibid, 20.
[29] Kerr (2014), 410.
[30] Ibid, 404.
[31] *re Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp*, Microsoft Reply Brief (July 24 2014), 6 (**the Microsoft Reply Brief**). An example provided is where US-based banks are compelled by subpoena to produce business records concerning when customers access their safety deposit boxes. If the deposit box is held by a foreign subsidiary, its *contents* (as opposed to business records about the deposit box) can only be accessed through MLA, and Microsoft argued the same should apply to its customers' emails.

its search powers of foreign computers, without a warrant.[32] Finally, it is quite arguable that there was a breach of the principle of non-intervention[33] through the execution of the request in Ireland, although this was not directly considered. While there is no explicit definition of the principle of non-intervention,[34] as discussed in chapter two, it clearly covers "incursion or exercise of governmental authority by a State on another State's territory, without that State's freely given and duly authorised consent,"[35] which seemingly occurred here (albeit through the actions of Microsoft). If Ireland had ratified the Convention,[36] it may have been arguable that it had permitted such seizures of data from its territory, particularly as the Explanatory Report to the Convention appears to recognise that Article 18(1)(a) can be used to remotely access data in this way.[37] However, a treaty cannot create rights or obligations for third States.[38]

All of this further illustrates the protean nature of the legal construct of territoriality, as discussed in chapter two. As Kerr notes, section 2703 of the SCA only applies inside US territory, but the execution of the warrant can be viewed as a territorial act (by focusing the location of the provider), or as an extraterritorial act (by focusing on the location of the data), and both are

[32] See *US v Gorshkov* [2001] WL 1024026 (WD Wash, May 23, 2001). This case is discussed below in section 4.2.3. The decision also contradicts a subsequent ruling of the Second Circuit's that the act of copying electronic files (which was done in Ireland) constitutes a seizure, even prior to access by the agent involved: *United States v Ganias* 12-240-R (2d, June 17, 2014).

[33] The decision has been widely interpreted as constituting a "breach of Irish sovereignty": see e.g. O'Connor (2014), 11 and 'Brief of *Amicus Curiae* Anthony J. Colangelo, International Law Scholar, in Support of Appellant', *Microsoft Warrant Case* (15 December 2014). Michael McDowell (a former Irish Attorney General) has also argued that Microsoft would not be able to rely on any of the data protection exemptions under Irish law and would thus be in breach of the Irish Data Protection Acts 1988 and 2003 (See O'Connor (2014)). Breach of foreign law has not, however, prevented the operation of US subpoenas pertaining to foreign data. See e.g. the operation of Bank of Nova Scotia subpoenas which have been used "to compel a bank that does business in the United States to turn over records held by a branch of the same bank in a foreign country, even where production of the records would violate the foreign country's secrecy laws": US Attorneys Criminal Resource Manual 279, title 9.

[34] Gill (2013), 221.

[35] Ibid, 222. See also Wood and Jamnejad (2009), 372: "[e]xamples of prohibited extraterritorial enforcement jurisdiction include the collecting of evidence … conducted without the consent of the territorial state."

[36] It signed the Convention in 2002 but has not ratified it.

[37] See para. 173 of the Explanatory Report to the Cybercrime Convention.

[38] Article 34 of the Vienna Convention on the Law of Treaties (1155 UNTS 331, 1969).

"plausible perspectives."[39] There is therefore a "mismatch [between…] the territorial statute and the global Internet."[40] The location of the provider, however, is assuming priority in the minds of US judges, which is further demonstrated by the ongoing case involving Facebook. The social networking giant is also challenging the execution of an SCA search warrant, which was served on it in relation to the contents of the profiles of 381 individuals suspected of fraud.[41] Jackson J. stated that "Facebook could best be described as a digital landlord, a virtual custodian or storage facility for millions of tenants and their information."[42]

These decisions also further demonstrate the powerful position of the US when conducting cybercrime investigations, given the density of the Internet's architecture in the US and the number of 'digital landlords' located there that have "possession or control"[43] of information pertaining to individuals across the world.[44] It has been argued that this exercise of power by the US government sets a precedent which would outrage the "American people" if the converse occurred, whereby a foreign government compelled a local service provider to produce information about, for example, a "New York Times reporter, a Member of Congress, or a federal judge."[45] This precedent, however, was already set in the Article 18(1)(a) of the Convention, which requires State Parties to implement this precise power. However, regardless of

---

[39] http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/07/07/what-legal-protections-apply-to-e-mail-stored-outside-the-u-s/ (Accessed 20/12/2014).
[40] Kerr (2014), 408.
[41] It is not known if these individuals are based in the US or abroad, or where the data from their profiles is stored. Facebook is challenging the proportionality of the privacy infringement in the case, given the trove of data revealed.
[42] *re. Search Warrants Directed to Facebook* (Undocketed decision of Jackson J., 17 September 2013, pg. 1, available at: http://www.nytimes.com/interactive/2014/06/26/technology/facebook-search-warrants-case-documents.html) (Accessed 20/12/2014). Emphasis added. The appeal is due to be heard in December 2014, with a decision expected in 2015. See http://www.nytimes.com/2014/09/26/nyregion/facebook-suit-over-warrants-can-proceed-court-rules.html?_r=0 (Accessed 20/12/2014).
[43] Article 18(1)(a) Cybercrime Convention.
[44] Many of the major providers such as Google and Facebook have more customers outside the US, than within: Kerr (2014), 406-7. The Internet's architecture also means domestic implementations of (or provisions which seek to comply with) Article 21 of the Convention (interception of content data) can result in powers which mean very different things in practice for different countries.
[45] Microsoft Reply Brief, *supra* note 31, 1.

where these providers are established, the US is not alone in being able to secure data directly from them, as the next section will demonstrate.

4.2.2. The Foreign Service Provider

While a country may place service providers based within its territory under any number of onerous obligations,[46] providers that have no domestic presence have traditionally been thought to be completely out of reach of domestic process,[47] and indeed some countries would regard it as a criminal offence for LEAs of a foreign country to contact service providers within their jurisdiction for information.[48] For many LEAs, however, the practical reality is very different.

LEAs routinely request—and are provided with—data from foreign service providers, without formal inter-State process such as MLA.[49] Information from these providers can be important for any criminal investigation, but is often critical to cybercrime investigations. Many service providers make provision in their privacy policies and terms of service for providing information to LEAs,[50] and can specifically mention compliance with foreign requests.[51] Indeed, some service providers, such as eBay[52] and Facebook,[53] have developed sophisticated online request systems, and can boast response times of within 3-5 days.[54] Accompanying guidance sets out the requirements for such requests, as well as

---

[46] See Articles 16-21 of the Convention.
[47] Mann (1984), footnote 82.
[48] Report of the Transborder Group, 'Transborder access and jurisdiction: what are the options?' (2012) T-CY 3, para. 118 (the **Report of the Transborder Group 2012**).
[49] SOCA Interviewee (3).
[50] An academic survey of standard terms and conditions used by cloud service providers revealed that they reserved the right to disclose customer data to law enforcement almost without exception. The specificity of these provisions varied widely, but can be in the broadest of terms, such as acting in the company's best interests. See Bradshaw, Millard, and Walden (2011).
[51] Facebook's Data Use Policy, for example, states that it may respond to "legal requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law in that jurisdiction…" See https://www.facebook.com/about/privacy/other (Accessed 20/12/2014). Only in relation to the "contents of an account" is it suggested MLA or letter rogatory is required: https://www.facebook.com/safety/groups/law/guidelines/ (Accessed 20/12/2014).
[52] https://lers.corp.ebay.com/AIP/portal/home.do (Accessed 20/12/2014).
[53] https://www.facebook.com/records/x/login/ (Accessed 20/12/2014).
[54] See e.g. eBay's Law Enforcement Portal and Law Enforcement Guide, available at: http://pics.ebaystatic.com/aw/pics/uk/safetycentre/Guide-eBayUnitedKingdom.pdf (Accessed 20/12/2014).

the types of information that can be obtained.[55] Analysis of these service providers' transparency reports reveals that such portals are very well utilised.[56] Broadly speaking, the information provided to LEAs through these channels is 'non-content', although even the contents of communications can be provided in exceptional circumstances, such as where it is a life or death situation.[57]

Some countries have certainly struggled to compel compliance from some service providers. The Belgian Yahoo! case, for example, involved a prosecutorial data request being sent directly to Yahoo! in the US, by Belgian prosecutors. Yahoo! did not have any establishments within Belgium but it was nevertheless argued that "Yahoo is territorially present in Belgium, both as a commercial entity and as a service provider, that is at least virtually through the Internet."[58] The case has gone through numerous appeals on various points of law, and is now before the Belgian Court of Cassation for a third time,[59] but the latest decision from the Court of Appeal upheld Yahoo!'s criminal conviction for non-compliance, finding that "Yahoo!'s presence in Belgium is territorial" [60] and the fact that Yahoo! "does not appear to have a headquarters in Belgium [was…] not relevant."[61] In other words, Belgian procedural rules on data production were found to apply to a foreign service provider, based on the fact that it offered its "webmail services in Belgium."[62]

Countries like the UK, however, have not faced such resistance. It is now openly acknowledged that many of the most prominent service providers, such as Hotmail, Google, Microsoft and Facebook, respond directly to LEA

---

[55] See e.g. http://pics.ebaystatic.com/aw/pics/uk/safetycentre/Guide-eBayUnitedKingdom.pdf (Accessed 20/12/2014).
[56] See e.g. Facebook's Global Government Request Report: https://www.facebook.com/about/government_requests (Accessed 20/12/2014).
[57] SOCA Interviewee (3). See also below note 70. For the definition of communications data in the UK, see s. 21(4) RIPA.
[58] Ghent Court of Appeal, (Case No. 252/09, 30 June 2010), [14]. Translated version provided by Jan Kerkhof, one of the Belgian Prosecutors involved in the case.
[59] A date for the hearing is not yet set (email communication with Jan Kerkhof, 12 November 2014).
[60] Court of Appeal of Antwerp, (Case No 2012/CO/1054, 20 November 2010), [4.4.1]. Translated version provided by Jan Kerkhof.
[61] Ibid.
[62] Ibid.

requests,[63] and some have acknowledged having an "extremely cooperative professional relationship"[64] with UK LEAs. At the time this comment was made in 2012, these relationships were said to entail "voluntary compliance with RIPA."[65] This was confirmed in my interviews with SOCA: "[a]t the moment we're using UK instruments to serve on US parties that actually don't have to comply. It's a working relationship, but they wouldn't be summon-able if they then turned around and refused to provide that data."[66] There were actually two reasons why this relationship was voluntary. First, many of these service providers were not, strictly speaking, offering 'telecommunication services' under RIPA.[67] The second—more obvious—reason as to why these relationships were voluntary, was because most of the service providers were not established in the UK, and thus not subject to a UK procedural instrument. There is something distinctly paradoxical about this paradigm: service providers maintain that their compliance is voluntary and fulfilling their social responsibility,[68] yet they insist on law enforcement following their own domestic authorisation processes to every last detail.[69] The legal explanation for this, and for how these transnational interactions began between (mostly US based) globally operating service providers and (often EU based) LEAs, is likely to be that under US law, service providers can divulge certain information pertaining to subscribers of their services in certain exceptional circumstances, including where the provider has the lawful consent of the subscriber (e.g. through agreement with terms and conditions).[70]

However, these transnationally operating service providers, processing personal data of EU citizens, are also clearly bound by EU data protection

[63] See e.g. the report of Joint Committee on the Draft Communications Data Bill (28 November 2012), paras. 230-3. Available at: http://www.publications.parliament.uk/pa/jt201213/jtselect/jtdraftcomuni/79/79.pdf (Accessed 20/12/2014).
[64] Stephen Collins of Microsoft, ibid, para. 232.
[65] Ibid.
[66] SOCA interviewee (3).
[67] For discussion in the context of social networking sites see O'Floinn and Ormerod (2011), 769.
[68] Comments of Stephen Collins, Microsoft, *supra* note 63.
[69] SOCA interviewee (3).
[70] See 18 U.S.C. § 2702(c)(2). Even 'content' information can be provided where there is a danger of death of serious injury: 18 U.S.C. § 2702(b)(8).

rules,[71] and require valid grounds for the processing of this data directly to LEAs. It may have been thought that this processing was legitimate for the purposes of EU data protection law, either because of their subscribers' consent (e.g. agreement to terms and conditions),[72] or because they were under a legal obligation (e.g. a RIPA request),[73] but neither are convincing grounds for processing in this context, as I have argued elsewhere.[74] Where RIPA requests were being complied with voluntarily, for example, it cannot be said that the processing was necessary for compliance with a legal obligation;[75] as Walden notes, "[w]hile the authorisation process itself may be 'in accordance with the law' [domestically], the act of serving it [abroad] may render it unlawful."[76]

4.2.2.1 Formalising compliance: RIPA and DRIP

These legal uncertainties (in particular the classification of service providers under RIPA, and compliance with data protection law) assumed greater importance after the Snowden revelations, as service providers' disclosure practices were put into the spotlight. In order to respond to these events, and maintain current levels of cooperation, the UK government seized the opportunity to amend RIPA when it introduced emergency legislation to address the striking down of the Data Retention Directive.[77] The Data Retention and Investigatory Powers (**DRIP)** Act 2014 addressed both of the legal uncertainties mentioned above. Section 5 extended the definition of "telecommunication service" by inserting a new provision (section 2(8A)) into RIPA.[78] Section 4, meanwhile, purported to extend the territorial reach of some of the procedural powers in RIPA, inserting provisions which allow for interception warrants and notices for communications data to be served on

[71] For an illustration of the jurisdictional scope of EU data protection rules, see Article 4 of the Data Protection Directive (95/46/EC of 23 November 1995) and its application by the CJEU in *Google Spain v AEPD* (Case C-131/12, 13 May 2014).
[72] Article 7(a) Data Protection Directive.
[73] Article 7(c) Data Protection Directive.
[74] O'Floinn (2013).
[75] See Schedule two, para. 3 of the Data Protection Act 1998.
[76] Walden (2013), 50.
[77] *Supra* chapter three, note 171.
[78] The precise parameters of this new definition are as yet unclear, and will depend on its interpretation in relation to particular services. However, the Explanatory Notes to the Act, para. 56 state that this new definition was explicitly meant to cover "companies that provide internet-based services, such as webmail."

persons outside the UK.[79] These orders can now relate to conduct outside the UK.[80] It is explicitly stated that service providers are placed under a duty to comply with such orders,[81] with non-compliance even exposing them to criminal penalties.[82] Therefore, the standard territorial extent provision in section 8 of the Act is clearly understating what is occurring here. In effect, the legislature is explicitly providing for what the Belgian prosecutor sought to do: extend the territorial reach of procedural powers based on service providers' virtual presence within the UK.[83]

Parliamentary debates reveal that this extraterritorial prescription of powers was aimed at "maintain[ing] the current situation."[84] The Home Secretary argued that relevant provisions of RIPA had always applied extraterritorially, and that section 4 was simply to put the status quo "beyond doubt."[85] Service providers were said to be "looking for"[86] the change, which, if true, means there may have been a realisation that the voluntary cooperation frameworks were potentially unlawful for data protection purposes. It was recognised that some foreign service providers may not cooperate, even with their duties being "spelled out explicitly",[87] and that the threat of sanctions would in many cases be an empty threat. But the government clearly sought to capitalise on the fact that the threat of sanctions is but one motivating factor for inducing compliance,[88] and the legislation would furnish results at least with those with whom domestic LEAs have existing relationships.

This is an unprecedented legislative move in the UK, but as emergency legislation these provisions received limited scrutiny, and the full ramifications

[79] Sections 4(2) and 8 DRIP Act 2014, amending sections 11 and 22 RIPA respectively.
[80] Section 4(1) DRIP Act 2014. As Smith observes, there was considerable uncertainty on how provisions of RIPA mapped onto location of conduct prior to these amendments: http://cyberleagle.blogspot.co.uk/2014/07/dissecting-emergency-data-retention-and.html (Accessed 20/12/2014).
[81] See ss. 11(4) and 22(6) RIPA, as amended by ss. 3(3) and 4(9) DRIP Act 2014.
[82] See e.g. s. 11(7) RIPA 2000, as amended by s. 4(7) RIPA.
[83] Malcolm Rifkind said during Parliamentary debates: "We are talking about companies that *operate within* the United Kingdom." Hansard 15 July 2014: Column 727. Emphasis added.
[84] Ibid.
[85] Theresa May, Hansard 15 July 2014: Column 709.
[86] Malcolm Rifkind, Hansard 15 July 2014: Column 727. See also para. 16 of the explanatory notes to RIPA which state "[t]hese companies argue that they will only comply with requests where there is a clear obligation in law."
[87] Malcolm Rifkind, Hansard 15 July 2014: Column 727.
[88] Kelsen (1946), 24 argues, for example, that motives for lawful behaviour can be due to moral or religious ideas which run parallel to the legal order.

may not have been appreciated. David Davis MP asked, for example, what the implications were of demanding extraterritorial powers over globally operating service providers and what would happen when "China, Russia and other unpleasant powers [begin] claiming the same power",[89] to which no answer was received. Neither did it appear to be recognised that in moving from a regime where service providers were voluntarily cooperating, to a regime where they were being 'compelled' to cooperate, the government was prescribing a system contrary to international law. The act of serving[90] such orders on foreign service providers, in a foreign country, under threat of civil and criminal sanction, would seem to unquestionably constitute an extraterritorial exercise of enforcement jurisdiction, and thus an infringement of the principle of non-intervention.[91]

The UK government has not been alone in its myopic pursuit of formalising transnational interactions between LEAs and foreign service providers. The Convention, in fact, may actually render some of these interactions lawful under international law,[92] and those behind the Convention's revision are intent on promulgating a reading of it that would further facilitate these transnational interactions.

4.2.2.2 Provisioning for the Foreign Service Provider in the Convention

As noted, Article 18(1)(b) of the Convention requires Parties to also create a service-in-territory production order, pertaining to subscriber information. Walden observes that a possible interpretation of this provision is that it may "mean that an order may be served where both entity and data reside in a foreign jurisdiction."[93] It is at least arguable that amongst States that have ratified the Convention, such transnational interaction with service providers

[89] David Davis, Hansard 15 July 2014: Column 709.
[90] This can be done by e.g. electronically sending the order: ss.11(2A) and 22(5B) RIPA.
[91] See Wood and Jamnejad (2009), 372, as discussed in chapter two, section 2.2. The Home Secretary even stated that the extraterritorial provisions were to "strengthen … the ability to *enforce* in this area." Theresa May, Hansard 15 July 2014: Column 709. Emphasis added. The UK itself previously implemented legislation to control such extraterritorial enforcement measures from other foreign countries in the Protection of Trading Interests Act 1980. For discussion, see Lowe (1981).
[92] See e.g. Article 18(1)(b).
[93] Walden (2013), 50.

was envisaged.[94] This interpretation, however, does not appear to be realised,[95] and the orthodox position seems to be that it requires countries to implement powers to order disclosure of subscriber information controlled by an entity, whether stored in the State or otherwise, but only if the entity is physically located in the State.[96]

4.2.2.3 The vexed Article 32(b)

An alternative source of authority for the interactions described above is sometimes said to exist in the Convention in Article 32(b). This allows a Party, without the authorisation of another Party, "to access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the *lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party*."[97]

This provision has its roots in the G8 Principles on "transborder access to stored data",[98] which is in substantially the same terms, except the Principles require searching States to "consider notifying the searched State, if such notification is permitted by national law and the data reveals a violation of criminal law or otherwise appears to be of interest to the searched State."[99] Even this shallow commitment wasn't maintained in the Convention.

Article 32(b) is a rather innocuous provision on first glance, but is the most controversial in the entire Convention, and widely known to be one of the main reasons for Russia's non-ratification. It has been described as the "most important provision on transborder access foreseen in the Convention",[100] was the result of protracted negotiations, but remains "often misunderstood."[101] This is not helped by the lack of publication of the *travaux préparatoires* to the

[94] However, even if Article 18(1)(b) was a permissive rule that allowed contacting a foreign service provider that was offering its services within the territory, it relates only to *subscriber* information. The DRIP Act 2014 pertains to a wider category of data, such as traffic data within the meaning of Article 1(d) of the Convention.
[95] It was not mentioned as a possibility, for example, in the Report of the Transborder Group 2012.
[96] This is apparently the position of the United States in relation to Article 18. Ibid, para. 235.
[97] Emphasis added.
[98] Released at the Ministerial Conference of the G8 Countries on Combatting Transnational Organized Crime, (Moscow, October 19-20, 1999).
[99] Ibid.
[100] Report of the Transborder Group 2012, para. 89.
[101] Ibid, para. 295.

Convention, although the drafters apparently deliberately left "'constructive ambiguity' so that it could address different situations."[102]

The principal points of contention concerning Article 32(b) are: a). whether a "person" can include a legal entity, such as a cloud service provider; b). whether the provision permits directly contacting a (legal) person when they are based in a foreign territory; and c). if the answer to b) is yes, the applicable law in relation to the words "lawful and voluntary consent" and "lawful authority to disclose." The Explanatory Report to the Convention provides little explanation or assistance on any of these issues, stating vaguely that "[w]ho is a person that is "lawfully authorised" to disclose data may vary depending on the circumstances, the nature of the person and the applicable law concerned."[103]

Nevertheless, it is commonly assumed that Article 32(b) does apply to legal entities, and that the request can be made transnationally. As noted, service providers' contractual agreements will frequently permit disclosure of information to LEAs at their discretion, and the argument is that this results in the service provider having "lawful authority to disclose the data" within the meaning of Article 32(b). The Comprehensive Study on Cybercrime, prepared by the United Nations Office on Drugs and Crime (**the UNODC Cybercrime Study**), states, for example, that:

> Article 32(b) conceivably applies in [a] wide range of circumstances, including accessing or receiving computer data from extra-territorial individuals; private sector organizations; service providers; and—in today's world—cloud service operators. A potential advantage of Article 32(b) to law enforcement is that, if lawful and voluntary consent is contained, investigators do not have to follow mutual legal assistance procedures that move too slowly for capture of transient data.[104]

This reasoning has its roots in a recent discussion paper drafted by the "Ad-hoc sub-group of the T-CY on jurisdiction and transborder access to data" (the

---

[102] Ibid, para. 95.
[103] Explanatory Report to the Cybercrime Convention, para. 294.
[104] UNODC Cybercrime Study (2013), 219. The group behind this study was created following a request by the General Assembly to the Commission on Crime Prevention and Criminal Justice (GA Resolution 65/230, para. 42). The study was based on information received from governmental actors in 69 States, 40 private organisations, 11 inter-governmental organisations, and 16 academic organisations.

Transborder Group).[105] In 2011, the Council of Europe's Cybercrime Convention Committee (T-CY) established the Transborder Group and tasked it with developing an instrument (e.g. an amendment to the Cybercrime Convention, a Protocol, or recommendation) to further regulate transborder access to data and data flows, and the use of transborder investigative measures on the Internet and related issues. Its proposals for a new protocol will be discussed below, but of relevance for present purposes is the Transborder Group's decision that "there is no need to amend Article 32 in its present form",[106] it being sufficient to issue a guidance note to assist countries in understanding the provision.[107]

In preparation for a public hearing on its proposals at the Council of Europe (which I attended) a draft of this guidance note was circulated.[108] This has since been revised on numerous occasions after aspects of the note were subject to staunch criticism at the public hearings.[109] Nevertheless, the final adopted version of the guidance note[110] gives an incredibly broad interpretation to each of the aforementioned contentious issues within Article 32(b), one which is most favourable to law enforcement conducting transnational enquiries. On the "person" that can consent to disclosure of data, the note suggests it can be a physical person, but also a legal person.[111] This may contradict the intention of the drafters. When questioned at the public hearing in June 2013, a current Bureau member that was involved in the original drafting of the Convention[112] admitted that she could not recall the issue of service providers granting consent to access data being discussed in the context of Article 32(b). This was a rare insight because, as mentioned in chapter three, the full makeup of the

[105] The members of the Group are mentioned in the Report of the Transborder Group (2012), 4, and they are all, I believe without exception, either current or previous criminal prosecutors or investigators. We will see that these biographical characteristics are strongly reflected in their proposed guidance notes and suggested protocol, discussed below.
[106] Ibid, para. 295.
[107] Ibid.
[108] T-CY Draft Guidance Note no. 3 'Transborder access to data (Article 32)', version 19 February 2013 T-CY (2013)7E.
[109] For a comment on the June 2013 hearing and further critique of the guidance note, see O'Floinn (2013). The guidance note was also critiqued at a hearing in December 2013, which I also attended.
[110] T-CY Guidance Note no. 3 'Transborder access to data (Article 32) (T-CY (2013) 7E, 3 December 2014) (the **Article 32 Guidance Note).**
[111] Article 32 Guidance Note, at para. 3.6.
[112] Betty Shave, USA.

drafting committee is not widely known. The admission also coheres with the examples of interactions envisaged in the Explanatory Report.[113]

On whether that person can be in a foreign territory, the guidance admits that "[t]he standard hypothesis is that the person providing access is physically located in the territory of the requesting Party. However, multiple situations are possible."[114] The guidance note specifically suggests that a legal person could be located in a third country when cooperating.[115] This contradicts the views of Henrik Kaspersen, the "father" [116] of the Convention who chaired the Committee of Experts on Crime in Cyber-space responsible for drafting the Convention.[117] Kaspersen previously stated that:

> [t]he person who co-operates with law enforcement authorities in the case of art. 32(b) is present in the territory of [the] investigating Party … and cannot be used to obtain co-operation of a person that does not fall under the jurisdiction of the investigating State.[118]

Members of the Transborder Group also seem to have quietly forgotten about provisions in the Council of Europe's own guidance which suggest that "domestic law enforcement authorities should be encouraged not to direct requests directly to non-domestic Internet Service Providers."[119]

Finally, on the words "lawful and voluntary consent" and "lawful authority", the guidance notes have been simply incoherent.[120] Contradicting its first note,[121] the guidance currently states that "[s]ervice providers are highly

---

[113] Explanatory Report to the Cybercrime Convention, para. 294. The examples provided include when an individual provides access to emails or data he has stored in a computer system in another country. This neither envisages a transnational request being possible.
[114] Article 32 Guidance Note, para. 3.8.
[115] Ibid.
[116] Schjolberg (2008), 2.
[117] Kaspersen (2006), 9.
[118] Kaspersen (2009), para. 81.
[119] Council of Europe, 'Guidelines for the cooperation between law enforcement and internet service providers against cybercrime' (2008), para. 36. Available at: http://www.coe.int/t/informationsociety/documents/Guidelines_cooplaw_ISP_en.pdf (Accessed 20/12/2014).
[120] For critique see O'Floinn (2013). Even the final Guidance Note fails to appreciate the distinction between consent for the purposes of data protection law (which is relevant to whether service providers have 'lawful authority' to disclose), and the service providers consenting to disclosure of data within the meaning of Article 32(b). See paras. 3.4 and 3.6 of the Article 32 Guidance Note.
[121] The February 2013 Guidance Note, *supra* note 108, para. 3.5, said "the person providing access may be an Internet or cloud service provider … if the terms of service or contract permit this."

unlikely to be able to consent validly and voluntarily to disclosure of their users' data."[122] The only reason provided for this is because "they will not control or own the data."[123] This conflates the authority to disclose with the issue of whether the service provider voluntarily consented.[124] It also implies that if the domestic law of the service providers was such that they did 'control' or 'own' the data, as in the *Microsoft Warrant* case, the information could be provided transnationally to foreign LEAs. The guidance note further suggests that the applicable law, where transnational interactions do occur, is the domestic law of the LEA. This would mean, for example, that if the LEA's domestic law contained an age of consent for these purposes whereby young children could cooperate, they could contact a child for his data in a foreign country, even if this would not be permitted in the country where the child is located. All in all, the Transborder Group's current efforts are clearly oriented towards further regularising LEA transnational interactions with foreign service providers, and providing a guise of legality for them. Even recent criticism of their work by the EU's Article 29 Data Protection Working Party, who argued that service providers could not provide data 'voluntarily' whilst remaining in compliance with data protection law, was rebuked:

> [there are] situations where an Internet Service Provider or another data controller could disclose data (emergency situations, controller becomes aware of an offence, ISP is attacked, *commercial rules,* etc.). The statement that a data controller can "never" voluntarily disclose data would not be correct.[125]

Therefore, the (supposedly) deliberate 'constructive ambiguity' in relation to Article 32(b) is being moulded to suit the interests of LEAs, which is very much in keeping with the trend of suppression conventions.[126] This wide interpretation is concerning for a number of reasons. First, unlike MLA where

---

[122] Article 32 Guidance Note, para. 3.6.
[123] Ibid.
[124] Article 32(b) cannot render lawful, under international law, the extraterritorial enforcement powers envisaged in the DRIP Act 2014, even where the service provider is in a country that is party to the Convention, as the service providers are threatened with civil and criminal penalties for failure to cooperate. On any interpretation of the word 'consent' in Article 32(b), such cooperation is not consensual.
[125] Transborder Group Report 'Transborder Access to Data and Jurisdiction: Options for Further Action by the T-CY' (T-CY 2014 16, 3 December 2014), para. 2.2.4. Emphasis added. The reference to 'commercial rules' is clearly an attempt to further a reading of Article 32(b) that allows law enforcement to directly liaise with foreign service providers for data, if their terms and conditions allows for this interaction.
[126] See chapter three.

there are pre-existing clear channels between States, the nature of the relationships between LEAs and foreign service providers can be *ad-hoc* and amateur. While some of the major service providers such as eBay and Facebook can provide secure communication channels, others simply respond to police requests originating from generic email accounts and have no secure mechanism for verifying the authenticity of the request, or communicating the data.[127] Second, their operation is opaque with no governance or oversight mechanisms. [128] Third, there are obvious privacy concerns [129] with these networking interactions and it is not clear how many of these service providers are currently purporting to comply with their EU data protection obligations; these issues were given scant attention by the Transborder Group.[130] Finally, this wide interpretation will continue the status quo whereby service providers decide with which countries they will cooperate (as their participation must be consensual under Article 32(b)), thus resulting in uneven distribution[131] and a restricted 'club' of LEAs that have access.[132] Some countries never receive positive responses for data requests to service providers,[133] and this not only hampers cybercrime investigations, but investigations and prosecutions of any criminal offences that may entail evidence from service providers. Moreover, these entities decide the circumstances when they will cooperate. A UK LEA reported to me that a service provider once refused to provide information in relation to a British citizen, concerning a serious crime committed in the UK, as the suspect was now in a foreign country when utilising the service. Others have much more permissive internal rules for cooperation, and will provide data pertaining to foreign suspects as well.

---

[127] This was confirmed in some of my interviews with service providers. See also Kent (2014), para. 50.3.
[128] This is also a broader concern with the operation of TGNs: Newman and Zaring (2013), 255.
[129] Domestic voluntary cooperative frameworks between LEAs and service providers have been found to be unlawful in Canada, with the Supreme Court ruling that a police request for the voluntary disclosure of communications data constituted a 'search' and a violation of s. 8 of the Canadian Charter of Rights. See *R v Spencer* [2014] SCC 43.
[130] See O'Floinn (2013).
[131] Raustiala (2002), 16.
[132] This is again also a broader problem with the operation of TGNs. They may be unevenly distributed, with restricted participation: Eilstrup-Sangiovanni (2009), 202.
[133] Google's Transparency Report reveals that 23 countries had a 0% response rate between January to June 2014. This includes Turkey—one of the latest countries to ratify the Convention—that had all of its 224 requests refused.

The difficulties which the Transborder Group have encountered in interpreting Article 32(b)—with fundamental differences existing between their various draft guidance notes—clearly suggest that this provision was not designed for the transnational interactions which it is now said to permit. But the motivation for attempting to read the provision so widely is clear; it would be unpalatable to most States to formalise such relationships clearly in an international provision, as it would necessarily entail foreign LEAs contacting domestic service providers directly, and could involve information about citizens being provided to countries that may not share similar values. Bringing current cooperative frameworks within the purview of Article 32(b) obviates the need for such formalisation, and maintains the efficiency of the status quo (for some countries), and the Transborder Group is not alone in its attempt to legally embed them. The Internet Corporation for Assigned Names and Numbers (**ICANN)** is also investigating LEA access to registrant subscription data from domain name registrars,[134] while Svantesson has overtly sought to build on globally operating service providers' selective cooperation, attempting to develop an "international law doctrine of selective legal compliance"[135] which would, *inter alia,* involve determining the principles and criteria for when intermediaries should cooperate with States.[136] Although "selective compliance is of course already happening on a practical level",[137] this is a startling suggestion, providing pride of place to the preferences of service providers, and it is not clear how it could form a doctrine of 'international law', since it would necessarily entail ignoring the laws of countries, which would preclude both an international agreement, or the 'doctrine' ever developing into a rule of customary international law.

Coupled with the developments in the UK discussed in the previous section, the foreseeable future is, therefore, likely to entail service providers being

[134] ICANN's Generic Names Supporting Organization (**GNSO**) chartered a working group on "Privacy and Proxy Services Accreditation Issues" on 31 October 2013, with one of the questions concerning the circumstances which would warrant access to registrant data by law enforcement agencies from privacy and proxy service providers. The group is due to publish its full recommendations on LEA requests in 2015.
For more see: https://community.icann.org/pages/viewpage.action?pageId=43983094 (Accessed 20/12/2014).
[135] Svantesson (2014).
[136] Ibid, 353.
[137] Ibid.

placed in the invidious and unenviable position of having to assess the legal validity of foreign LEA requests for data (which they are in no position to do), and having to decide with which countries they will co-operate in this way. Countries that have power and influence over these providers, and that are deemed to share their values, will continue to reap the benefits of these relationships. The result is a further clustering of countries that have the ability to conduct cybercrime investigations, and a further obfuscation of the concept of territoriality in the context of enforcement jurisdiction.

4.2.3. Search and Seizure

Article 19 of the Convention requires that State Parties adopt measures to allow for the search and seizure of computer systems, and computer data stored therein, within its territory,[138] and to extend searches from one computer system to another in its territory, if it has grounds to believe the information sought is stored there and is lawfully accessible from or available from the initial system.[139] A range of measures, such as a seizure of the computer system, and copying of the computer data, are specifically enumerated.[140] This search and seizure power is most typically thought to concern law enforcement entering a suspect's home and seizing his hard-drive, which is obviously a powerful investigative tool that is well utilised by LEAs in cybercrime investigations.

The actual operation of domestic search and seizure powers reveals that Article 19 does not currently[141] cater for what is happening on the ground, limited as it is to searching data stored in computers systems on the searching State's territory, or other systems accessible from the searched system, if the former is also within the territory.[142] The reality is that searches of suspects' Internet-connected laptops and mobile phones will frequently involve accessing computer systems in other countries, but investigators,[143] academics,[144] and

[138] Article 19(1).
[139] Article 19(2).
[140] Article 19(3).
[141] See, however, the discussion of the proposed Protocol, below section 4.3.
[142] See also the Explanatory Report to the Cybercrime Convention, para. 193.
[143] See discussion of the two mobile phone search cases below, section 4.2.3.1.

even legislation[145] will often fail to recognise, or ignore, these territorial complexities. As with the *Microsoft Warrant* case, the territoriality of actions is again obfuscated by the networked environment, with practical and theoretical difficulties emerging in determining where searches occur, and when they may involve accessing data stored in foreign countries.

4.2.3.1 Mobile Phone Illustrations

Although not involving cybercrime investigations, two recent cases from either side of the Atlantic reveal how routine search and seizure powers can now entail transnational transgressions. Both cases involved seizures of mobile phones and the police powers to access data from those devices without search warrants. In *JL and EL*,[146] a Scottish case, police had detained two individuals for questioning in relation to an assault, and took possession of their smartphones, accessing, *inter alia*, text messages and Facebook communications. *Riley v California*,[147] a decision of the US Supreme Court, involved two cases with similar facts to *JL and EL*. In both cases, police tried to rely on exceptions to warrant requirements, pointing to common law powers of search after arrest.[148] In the Scottish case this was successful, with the High Court equating a mobile phone with a paper diary, both of which can be seized and analysed following arrest.[149] Little over a month later, the US Supreme Court, on the other hand, roundly dismissed such analogies, finding it was "like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies

---

[144] Sommer (2012), for example, argues that provided a search warrant is obtained, it would be unproblematic for a police officer to 'guess' the password of a suspect's account where he remotely stores information. It may be true that such a search would not involve the officer incurring criminal liability domestically, due to s.10 Computer Misuse Act 1990, but this provision could not absolve him from an offence committed in the jurisdiction where the data is stored (if this occurred). Sommer neither recognises that this may involve the extraterritorial exercise of enforcement jurisdiction if the data was stored abroad.

[145] Section 20(1) Police and Criminal Evidence Act 1984 (**PACE**), as amended, for example, provides that where officers have entered a premises and are exercising powers of seizure under the Act, they also have the "power to require any information stored in any electronic form and *accessible from the premises* to be produced in a form in which it can be taken away…" Emphasis added.

[146] *JL and EI* [2014] HCJAC 35.

[147] *Riley v California* [2014] 573 US.

[148] Although the appellants in *JL and EL* had not been arrested, s.14(7) of the Criminal Procedure (Scotland) Act 1995 provided a similar search power in the case of detentions.

[149] *JL and EI* [2014] HCJAC 35, [11].

lumping them together."[150] The Supreme Court recognised that seizure of mobile phones raised privacy concerns that were quantitatively and qualitatively different from seizure of other physical objects, and held that the Fourth Amendment generally required a search warrant for such inspections.[151]

I am not here concerned with comparing the privacy or warrant regimes in the US and Scotland, but with the fact that in both cases, data was accessed which may not have been stored in the investigators' territories. Chief Justice Roberts, who delivered the opinion of the US Supreme Court, acknowledged that a further justification for a warrant was that by accessing a suspect's phone and accessing applications by tapping its screen, the search may no longer be of data held in the device itself but involve the display of data stored remotely, and "officers searching a phone's data would not typically know whether the information they are viewing was stored locally … or has been pulled from the cloud."[152] In *JL and EL,* this fact was actually at the heart of the appeal, with one of the appellants arguing that accessing the Facebook application involved accessing "virtual material" [153] and constituted an interception of communications.[154] In the end, this issue was not addressed due to the way the points of appeal were constructed and because it involved matters of fact that had not been the subject of findings at first instance.[155]

4.2.3.2 When Searches Constitute Exercises of Extraterritorial Enforcement Powers

While it was appreciated in both cases that data accessed by searching a mobile phone could involve data stored remotely, neither judgment mentioned the potential international law complications. In *JL and EL* it is highly likely that the data 'pulled' pursuant to the search was stored extraterritorially and search warrants that are now issued in the US, post-*Riley*, for searching suspects'

[150] *Riley v California* [2014] 573 US, 17.
[151] Certain exceptions to the need for warrants, such as in order to prevent imminent serious injury, were noted. Ibid, 26.
[152] Ibid, 21.
[153] *JL and EI* [2014] HCJAC 35, [8].
[154] For an analysis of interception offences in the context of viewing social networking site material, see O'Floinn and Ormerod (2011), 783-6. See also *R v Coulson* [2013] EWCA Crim 1026.
[155] *JL and EI* [2014] HCJAC 35, [9].

phones, will undoubtedly involve data stored outside the US in some cases. Since the data in these cases were not publicly accessible,[156] it raises the question of whether such acts—or any search of a networked device which can be accessed during physical searches—actually constitute *acts* in foreign territories and an extraterritorial exercise of enforcement powers? Some States appear to assume they do not, or perhaps that other States must consent to such searches and that a customary rule of international law has developed in this regard. Article 15(5) of the Portuguese Law on Cybercrime,[157] for example, is said to go beyond Article 19(2) of the Convention, in that it allows a Portuguese LEA to access data in a remote system, which is stored in a foreign State, provided a valid search order is obtained and the data is "lawfully accessible from the initial system."[158] Presumably this means that if a search warrant is obtained, and a device is logged in, or the password is found or compelled by law,[159] Article 15 permits accessing the data, regardless of where it is.

Other States, however, may regard such activities as constituting an interference with their territorial sovereignty. In the *Gorshkov-Ivanov* case, for example, the FBI created a bogus computer security company and lured two computer hackers (Gorshkov and Ivanov) from Russia to the US for 'interviews' with the company. Both were asked to demonstrate their skills by hacking into a network set up by the FBI, which they did through accessing their own computer systems in Russia via the Internet. A keystroke logger was installed on the laptops used, which enabled the FBI to then access the Russian computers, download incriminating evidence, and prosecute the defendants. The defendants claimed this constituted a breach of Russian search and seizure laws, and that the evidence should have been excluded as it was without a warrant and violated the Fourth Amendment. The District Court rejected these

[156] Article 32(a) of the Convention sanctions accessing open source data, regardless of where it is located, but a customary international law rule has no doubt also emerged in this regard.
[157] Law No. 109/2009, of 15 September 2009 (Cybercrime Law). A translation of the law is available here: http://www.wipo.int/wipolex/en/text.jsp?file_id=206634 (Accessed 20/12/2014).
[158] Ibid, Article 15(5). This law is discussed at some length in the Report of the Transborder Group (2012), paras. 196-213, where it is stated that accessing data from webmail accounts, stored abroad, is envisaged. Ibid, para. 200.
[159] See e.g. s.49 RIPA.

arguments as the Fourth Amendment did not apply abroad, and the Russian search and seizure law did not apply to the agents' conduct.[160] The Russian government, however, was apparently enraged by the action,[161] and indicted the FBI agent on a hacking charge in Russia, sending a request for his extradition, to which the US has apparently never responded.[162]

Legal scholars have assumed that "Russian territorial sovereignty was violated by the United States in the *Gorshkov-Ivanov* case"[163] which, if correct, would also appear to apply to cases like *JL and EL*. Both involve suspects in the investigating State, and data controlled by them,[164] which is stored in another country, and accessed without their consent and without a search warrant. It is true that in the *Gorshkov-Ivanov* case, the suspects had more control of the data and knowledge of where it was located,[165] but it is not clear how or whether this could be sufficient to distinguish the cases for the purposes of determining whether there was a breach of the principle of non-intervention.[166]

Moreover, if cases like *Gorshkov-Ivanov* are not regarded as a territorial interference, then it may be more difficult to differentiate more serious transnational search techniques, where suspects may not know that searches occur, such as when LEAs gain remote access to suspects' computers. Brenner provides a basic definition of what this entails: "in its simplest formulation, a remote computer search is one in which the searchers are in a physical location other than the location where the computer that is the target of their search is situated."[167] This can clearly be done if police have access to the computer and can install physical keyloggers, but can also involve software that is covertly

---

[160] *US v Gorshkov* [2001] WL 1024026 (WD Wash, May 23, 2001). For further discussion of this case see Brenner and Schwerha (2002) and Seitz (2005).
[161] Brenner (2014), 53.
[162] Ibid.
[163] Seitz (2005), 49.
[164] Although in the mobile phone case, it will also be partly controlled by a third party, such as Facebook.
[165] In the case of mobile phone applications such as Facebook, the data will also be partly controlled by a third party, and the location of the data determined by them, rather than the individual alone.
[166] The nationality of the suspects cannot be relevant to whether the searches were extraterritorial or not, although it undoubtedly played a part in Russia's resistance to the operation.
[167] Brenner (2012), 61.

installed.[168] Cybercriminals are not the only ones that can utilise malware, and the FBI is known to have been using various remote data gathering programs for many years.[169]

Brenner has argued that using Trojan Horse programs like this in the US, could be a constitutionally permissible form of investigative work, provided a search warrant has been obtained authorising the specific activity.[170] Within Europe, the issue has also been addressed by the Federal Constitutional Court of Germany, which ruled in 2008 that such technologies could be utilised in exigent circumstances, such as where there is a threat to life.[171] This suggests fairly limited circumstances where remote searches could be utilised in Germany, but claims arose in 2011 that some German States were going far beyond what was permitted by the Federal Court.[172] It is reported that lower courts have sanctioned the use of Trojans on suspects' computers at least 50 times,[173] and that German Federal Police (the Bundeskriminalamt) has held meetings with various law enforcement agencies concerning the deployment of such monitoring software.[174] There is also some evidence that the UK has utilised remote search techniques.[175]

---

[168] Sommer (2012), 169.
[169] For discussion see Abel and Schafer (2009) and Soghoian (2010).
[170] Brenner (2012).
[171] http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007en.html (Accessed 20/12/2014). Headnote, [2].
[172] http://www.spiegel.de/international/germany/the-world-from-berlin-electronic-surveillance-scandal-hits-germany-a-790944.html (Accessed 20/12/2014) and http://www.nytimes.com/2011/10/15/world/europe/uproar-in-germany-on-police-use-of-surveillance-software.html?_r=0 (Accessed 20/12/2014). For discussion of the legislation which purportedly authorised this at the Federal level see: http://www.statewatch.org/analyses/no-79-germany-permanent-state-of-preemption.pdf (Accessed 20/12/2014).
[173] http://www.spiegel.de/international/germany/trojan-trouble-the-shady-past-of-germany-s-spyware-a-792276.html (Accessed 20/12/2014).
[174] http://www.slate.com/blogs/future_tense/2012/04/03/bundestrojaner_finspy_u_s_officials_met_with_germany_to_discuss_computer_surveillance_.html (Accessed 20/12/2014).
[175] It was reported in 2009 that the Home Office had adopted a new plan to allow police to practice 'remote searching' techniques. See http://www.timesonline.co.uk/tol/news/politics/article5439604.ece (Accessed 20/12/2014). A spokesman for the Association of Chief Police Officers once also confirmed that 194 hacking operations were carried out in 2007/8 in England, Wales and Northern Ireland, including 133 in private homes, 37 in offices and 24 in hotel rooms, with the searches apparently authorised by RIPA. See http://www.independent.co.uk/news/uk/home-news/new-powers-for-police-to-hack-your-pc-1225802.html (Accessed 20/12/2014). These were presumably authorised as intrusive surveillance, under s.32 RIPA, and s.93 of the Police Act 1997, as an interference with property.

Debates concerning the need and proportionality for such investigative techniques are just beginning, but a more pressing issue, from an international law perspective, is whether such remote searches are being done transnationally. A note circulated by the EU Council Presidency in 2008 stated that some "projects were already in existence" and that "common approaches" were required in "the area of remote computer searches, which are a *delicate issue because of their cross-border nature*."[176] As Bunyan notes, "[r]eading between the lines the phrase: 'projects already in existence' implies that State agencies in some Member States are already conducting cross-border remote computer searches in their home countries and across borders in other states."[177] The interior Ministers at the G6 meeting in Bonn in 2008 also discussed the concept of remote searches, stating that:

> all partner countries have or intend to have in the near future national laws allowing access to computer hard drives and other data storage devices located on their territory. However, the legal framework with respect to transnational searches of such devices is not well-developed. The interior ministers will therefore continue to seek ways to reduce difficulties and to speed up the process in future.[178]

The comment that the legal framework on transnational searches is not well developed is, to say the least, an understatement. Nevertheless, six years on, we are seeing signs that States are both exercising, and seeking to legislate for, such transnational search powers.

In May 2014, Dutch police admitted to hacking a server in relation to an investigation involving Blackshades malware, despite not knowing where the server was located.[179] Oerlemans has argued that such search powers could not

---

[176] EU Council Presidency Note, 'Comprehensive Plan to Combat Cyber Crime', 11784/08 (11 July 2008), 4. Emphasis added. Available at: http://www.statewatch.org/news/2009/jan/eu-remote-computer-access-11784-08.pdf (Accessed 20/12/2014).

[177] http://www.statewatch.org/analyses/no-83-remote-computer-access.pdf (Accessed 20/12/2014). The EU Council also previously adopted conclusions inviting Member States and the Commission to introduce measures which would facilitate "remote searches if provided for under national law, enabling investigation teams to have rapid access to information, with the agreement of the host country." See 'Concerted Work Strategy and Practical Measures Against Cybercrime', 2987th Justice and Home Affairs Council meeting, Brussels, 27-28 November 2008. No such measures have, however, been introduced.

[178] http://www.statewatch.org/news/2008/nov/g6-usa-sep-08.pdf (Accessed 20/12/2014).

[179] www.om.nl/vaste-onderdelen/zoeken/@85963/wereldwijde-actie/ (Accessed 20/12/2014). See also: https://blog.cyberwar.nl/2014/10/in-early-2015-dutch-govt-will-ask-parliament-to-grant-hacking-power-to-law-enforcement/ (Accessed 20/12/2014).

be authorised domestically, let alone transnationally,[180] strengthening his legislative analysis by pointing to the fact that a Cybercrime Bill will be debated in early 2015 in the Netherlands to regulate such hacking activities domestically, which would be superfluous if the power already existed.[181]

The FBI has also explicitly sought a search warrant to install data extraction software on a computer whose location was apparently unknown, but highly likely to be in a foreign country as one of the other computers involved had an IP address which resolved to a foreign country.[182] The software would have allowed complete access to the hard-drive of the target computer and allow the FBI to activate the computer's built-in camera. The government, however, needed to establish that the search would occur within the Southern District of Texas (where the warrant was sought) and its territorial argument to this end was essentially that "because its agents need not leave the district to obtain and view the information gathered from the Target Computer, the information effectively becomes 'property located within the district.'"[183] This was rejected by Smith J. who pointed to the fact that a search in a location outside the District would have occurred before the information could be accessed, and that this "search takes place, not in the airy nothing of cyberspace, but in a physical space with a local habitation and a name."[184] However, Smith J did recognise the potential utility of such techniques and said there may be "good reason to update the territorial limits of [search powers] in light of advancing computer search technology."[185]

It did not take long for proposals to emerge to this end. Little over a year later, the US Committee on Rules of Practice and Procedure[186] has proposed an

[180] http://leidenlawblog.nl/articles/hacking-without-a-legal-basis (Accessed 20/12/2014).
[181] Ibid. This Bill would apparently allow LEAs to "break into servers located abroad, if they were being used to block services." See http://www.bbc.co.uk/news/world-europe-22384145 (Accessed 20/12/2014) and for discussion of some of the background behind the Bill, see http://leidenlawblog.nl/articles/the-advent-of-cross-border-remote-searches (Accessed 20/12/2014).
[182] *re Warrant to Search a Target Computer at Premises Unknown* [2013] 958 F. Supp. 2d 753 (S.D. Tex), 753.
[183] Ibid, 757.
[184] Ibid, 759.
[185] Ibid, 766.
[186] 'Preliminary Draft of Proposed Amendments to the Federal Rules of Appellate, Bankruptcy, Civil, and Criminal Procedure' (August 2014). Available at:

amendment to Rule 41 of the Federal Rules of Criminal Procedure, which deals with search and seizure. One of the proposed amendments concerns the issuance of search warrants to allow:

> remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if: (A) the district where the media or information is located has been concealed through technological means.[187]

If this provision is ultimately debated solely from a domestic perspective, it may well be passed. Brenner has previously analysed such searches between US States, and considered the various forms of dissonance which can eventuate, for example, where different States have different levels of privacy protection. No dissonance is said to arise, however, if all states "use the same, federal standard: Remote searches are constitutional if they are conducted in accordance with the fourth amendment."[188] If officers in one US state conducted a remote search in another state, "the person who is the target of such a search … cannot move to suppress the evidence obtained in the remote search either on the grounds that it violated the Fourth Amendment or the law of either of the states involved."[189]

This may well be an accurate analysis of US constitutional law. However, somewhat problematically, Brenner also attempts to extend her discussion to the international plane, using the same concepts.[190] Her notion of rule dissonance is useful in capturing the difficulties which emerge where one State allows remote searches, while another does not, and/or where both countries have different privacy protections. But it neglects the fact that such extraterritorial searches would constitute the enforcement of State power in another country. The Committee's proposed amendment also neglects these extraterritorial implications; if the location of the computer were unknown, this would inevitably involve sanctioning search and seizure of computers and data outside the US (not simply outside of US Districts). Nor does it consider what

---

http://www.uscourts.gov/uscourts/rules/preliminary-draft-proposed-amendments.pdf (Accessed 20/12/2014).
[187] Ibid, Proposed Rule 41(b)(6)(A).
[188] Brenner (2012), 63.
[189] Ibid, 64.
[190] Ibid, 80-92.

it might mean for the media to be 'concealed', which could of course be interpreted widely.

Remote transnational searches or accessing suspects' data stored extraterritorially directly from their devices (without their consent), are not envisaged in the Convention, but if such developments were to be addressed by an institution such as the Council of Europe, one might expect a sophisticated discussion of the human rights and international law implications entailed. Instead, we will see that the suppression steam train is actually promoting such LEA activities with little thought to such concerns; in fact, the Transborder Group is advocating a protocol that would sanction a range of such transnational search powers.

4.3 The Proposed Protocol

Beyond the guidance note for Article 32(b), the work of the Transborder Group has been dedicated to proposing a new Protocol to the Convention to allow for "additional possibilities for transborder access to data",[191] (the **Draft Protocol**). To this end, the Transborder Group has published five proposals for possible elements of such an instrument which have been discussed, *inter alia,* at the June and December 2013 hearings at the Council of Europe, which I attended. Despite the best intentions of the organisers in maintaining a structured dialogue on each of these proposals, the conversation was scattered. This was partly because two of the proposals[192] significantly overlapped with the previous discussion concerning Article 32(b), but the primary reason seemed to be that the breadth of the proposals left participants somewhat incredulous, and much time was spent grappling with what was actually being proposed.

The first proposal was for "transborder access with consent without the limitation to data stored 'in another Party.'"[193] The drafters were here

[191] Ad-hoc Subgroup on Transborder Access '(Draft) elements of an Additional Protocol to the Budapest Convention on Cybercrime regarding Transborder Access to Data', T-CY (2013) 14, (version 9 April 2013).
[192] Proposal 1: 'Transborder access with consent without the limitation to data stored "in another Party' and Proposal 5: 'The power of disposal as connecting legal factor.'
[193] Draft Protocol, 5.

concerned with the "loss of location" which has (apparently)[194] eventuated in the networked environment, and the difficulty of knowing where data actually resides. Article 32(b) is restricted to data that is "located in another Party", and the Transborder Group were trying to cover situations where the data was stored in a non-Party, or the location was unknown. One of the difficulties with this, as the text of the proposal itself acknowledges, is that a treaty cannot create rights or obligations for third States.[195] Another concern is that they are suggesting widening Article 32(b) (e.g. losing the restriction that the data has to be located 'in another Party'), without it being clear what the existing provision actually currently covers, hence the need for the guidance note which, as discussed, has provided little actual guidance on many fundamental issues, or guidance which is textually highly questionable.

The second proposal was to provide for "transborder access without consent but with lawfully obtained credentials."[196] Even after the proceedings it wasn't entirely clear what was in mind with this proposal, but it would presumably cover a situation where an individual's email or social networking site password was acquired as part of an authorised covert surveillance operation, which is then used to access the accounts. It could obviously apply to situations where both the suspect and the data are abroad, and even if such a search was authorised domestically this could constitute a computer access offence in the country where the data is located.

However, it is the third and fourth proposals that are most alarming. The third provides for "transborder access without consent in good faith or in exigent or other circumstances."[197] This was rightly described by the representative from European Digital Rights (**EDRi**) at the June Hearing as a Pandora's box. It seems to suggest that States create domestic procedural powers so that an LEA could hack into a foreign computer system, if it was thought necessary to, for example, "prevent physical harm … [or] destruction of relevant evidence."[198]

---

[194] This is typically associated with the advent of cloud computing, but this overlooks the fact that even if information is scattered across numerous territories, the cloud service provider will normally know where it is, as in the *Microsoft Warrant* case.
[195] Vienna Convention on the Law of Treaties, *supra* note 38.
[196] Draft Protocol, 5.
[197] Ibid.
[198] Ibid.

This proposal appears to draw on doctrines of hot pursuit, with little recognition of the difficulties which exist when such power is exercised domestically,[199] let alone transnationally.[200]

The fourth proposal is equally startling. Article 19(2) of the Convention, as mentioned, requires Parties to legislate for extending searches from one computer system to others in its territory, when the data is lawfully accessible or available from the initial system. The Transborder Group said it "may be conceivable to drop"[201] the limitation that the latter computer system had to be in its territory. But given the architecture of the networked environment, data held *anywhere* could be 'available' to a computer system in any given country. The Pandora's box point is obviously also relevant here, as it would permit the types of remote searches conducted by the Dutch police in the Blackshades case, and more.

The fifth and final proposal—the power of disposal as connecting legal factor—was barely discussed at the June and December hearings. Again, it was the 'loss of location' of data which was of concern, and the provision suggests that "if the location of the data is not known, but the person having the power of disposal of the data is physically on the territory of, or a national of the searching Party, the LEA of this Party may be able [to] search or otherwise access the data."[202] This seems to envisage the exercise of powers as in cases like *JL and EL*, but would also permit States to directly access the data of its nationals, even when the person and data are abroad, if, for example, "access credentials have been lawfully obtained."[203] It prioritises nationality over sovereign territorial considerations and LEAs could no doubt readily claim that the location of data is unknown. Therefore, this raises the same concerns as some of the previous proposals, such as the fact that it would entail creating

[199] See in the context of warrantless house searches, *Kentucky v King* [2011] 131 S. Ct. 1849.
[200] See Gilmore (1995), on the operation of hot pursuit in international waters, which is permissible in tightly circumscribed circumstances under e.g. Article 23(2) Geneva Convention on the High Seas 1958. On the limited 'hot pursuit' border crossings permissible in the Meuse-Rhine Euroregion, see Hufnagel and McCartney (2014), 115. See also Article 41 Convention Implementing the Schengen Agreement 1990 (OJ L 239, 2000, p. 19), which allows for hot pursuit in carefully prescribed circumstances within the Schengen area.
[201] Draft Protocol, 5.
[202] Ibid, 6.
[203] As with the second proposal, it is not clear what is in mind with these words.

obligations for third States. Indeed, this proposal is so broad that it could range from access to data in cases like *JL and EL,* to instances like the *Microsoft Warrant* case, or even transnational requests to service providers, depending on how 'power of disposal' is interpreted or subsequently defined.

The Transborder Group is not alone in its efforts to expand the enforcement powers of cybercrime investigators.[204] The drafters of the UNODC Cybercrime Study are also concerned that the "traditional means of formal international cooperation in cybercrime matters is [sic] not currently able to offer the timely response needed for obtaining volatile electronic evidence"[205] and argue that the "role of evidence 'location' needs to be reconceptualized, including with a view to obtaining consensus on issues concerning direct access to extraterritorial data by law enforcement authorities."[206]

Therefore, the dominant discourse in the Council of Europe, and within key UN groups, is not to reconsider and improve international cooperation and the streamlining of preservation powers; the dominant discourse is to transform concepts of territoriality in the realm of enforcement and procedural powers. Lowe once observed that '[t]he most interesting question regarding the principle of non-intervention in international law is why on earth anyone should suppose that it exists."[207] Cybercrime investigations have forced this question to centre stage, with many seemingly supposing it should not, at least in the realm of their investigative work.

4.4 The Role of TGNs

I have already noted the increasing role of TGNs across all factions of governmental activities and some of the advantages and characteristics of TGNs, as opposed to traditional international cooperation: interaction tends to be informal and based on trust[208] and functional and flexible peer relationships; in structure, they are usually characterised by lateral ties and decentralised

[204] It has, however, been recently accepted that adopting its proposed protocol would be "controversial in the current context." Transborder Group Report 2014, *supra* note 125, para. 3.2.
[205] UNODC Cybercrime Study (2013), Key Findings and Options, xi.
[206] Ibid.
[207] Lowe (1994), 67.
[208] Eilstrup-Sangiovanni (2009), 200.

decision-making; and decisions do not create any binding international legal obligations for States.[209] Through their transgovernmental networking with foreign counter-parts, LEAs have found another significant way of extending their global reach. Numerous channels are available to LEAs in the EU, including Interpol,[210] Europol, or direct contact with foreign agencies.[211] Less known has been the role of 'liaison officers', who are now playing an important part in modern policing.[212] These individuals are posted in foreign countries, usually in embassies or consulates, on behalf of their country's agency, in order to liaise with law enforcement in the host country. They facilitate requests to, and from, their home country, and basically oversee "a hodgepodge of matters",[213] ranging from transmitting formal MLA requests, to facilitating the transfer of more informal information and communications. As Hufnagel and McCartney note, "cooperation has to be governed by informality to increase efficiency."[214]

The use of liaison officers as a tool for bilateral cooperation is recent,[215] but it is a phenomenon that has exploded in use, with both the US[216] and EU countries[217] setting up hundreds of liaison posts abroad. Europol alone hosts approximately 157 liaison officers,[218] including over thirty non-EU liaisons[219]

---

[209] Verdier (2009), 118. As discussed in chapter one, TGNs are found across all factions of governmental activities and can range from bilateral police networks to more institutionalised organisations, such as the Global Prosecutors E-Crime Network, or the Financial Action Task Force.

[210] On the legal foundations of Interpol, see Martha (2010). On the role of Interpol in policing transnational crime, see Hufnagel and McCartney (2014).

[211] Some organisations, such as the EU's Eurojust (which will be discussed in chapter six) share characteristics of both a traditional intergovernmental organisation and a TGN, but I agree with Eilstrup-Sangiovanni (2009), 198 that "TGNs and IGOs [intergovernmental organisations] are not mutually exclusive. Many IGOs are underpinned and complemented by TGNs."

[212] For an excellent analysis of the expansion of the use liaison officers (also known as legal attachés or LEGATs) by the US, see Nadelmann (1993). From a European perspective see Bigo (2000) and Block (2010).

[213] Nadelmann (1993), 152.

[214] Hufnagel and McCartney (2014), 110.

[215] The FBI sent its first liaison officer abroad in 1939 (Nadelmann (1993), 151), with European countries seemingly not latching onto the practice until 1971 when France sent a liaison officer to Washington (Bigo (2000), 76).

[216] Andreas and Nadelmann (2006), 170. For example, the US Immigration and Customs Enforcement currently alone has 75 offices in 48 foreign countries. See http://www.ice.gov/about/offices/homeland-security-investigations/oia/ (Accessed 20/12/2014).

[217] Block (2010), 199-200.

[218] https://www.europol.europa.eu/content/page/our-people-19 (Accessed 20/12/2014).

who form a particularly extensive and collaborative network, facilitated by their colocation in The Hague. Being unsupervised directly by Europol, they have ample scope for harnessing informal cooperation with their counterparts,[220] beyond the work of National units and Europol.[221] Therefore, as Andreas and Nadelmann note,

> [n]o longer do police plead in vain, as they did just a few decades ago, to be allowed to communicate directly across borders instead of via foreign ministries and consulates. Transgovernmental enforcement networks are more expansive and intensive than ever before, encouraging and facilitating a thickening of cross-border policing relationships.[222]

Cybercrime investigators have been able to build on this pre-existing web of relationships and networks that were established to tackle areas such as drug trafficking. A number of taskforces targeting specific types of cybercrime have been established, such as the Virtual Global Taskforce,[223] and very recently (September 2014), the Joint Cybercrime Action Taskforce (**J-CAT**), which is hosted at EC3 and already includes eleven countries (both EU and non-EU). These TGNs will work "side-by-side"[224] as "stakeholders in our global village,"[225] according to the Head of EC3 Troels Oerting. And they can already boast successes, including most recently 17 arrests involving dark markets that utilise the TOR network, such as the Silk Road. This particular operation (Onymous) was supported by J-CAT, and involved 16 European countries and the US;[226] such global operations and success stories are becoming increasingly common.[227]

---

[219] Most US LEAs have liaisons at Europol: https://www.europol.europa.eu/content/page/staff-statistics-159 (Accessed 20/12/2014).
[220] Mitsilegas (2009), 165.
[221] Article 8 of the Europol Decision (2009/371/JHA, 6 April 2009).
[222] Andreas and Nadelmann (2006), 232.
[223] This is an alliance of LEAs from ten countries, as well as Interpol and Europol, and numerous private sector partners, who attempt to tackle online child sexual exploitation and abuse.
[224] https://www.europol.europa.eu/content/expert-international-cybercrime-taskforce-launched-tackle-online-crime (Accessed 20/12/2014).
[225] Ibid.
[226] https://www.europol.europa.eu/content/global-action-against-dark-markets-tor-network (Accessed 20/12/2014). See also the achievements of the Virtual Global Taskforce, e.g. Operations Avalanche, Ore, and Buccaneer.
[227] See e.g. the Blackshades Malware Takedown, which involved 19 cooperating countries, and over 100 arrests worldwide: http://www.fbi.gov/news/stories/2014/may/international-blackshades-malware-takedown/international-blackshades-malware-takedown (Accessed

The nature of cybercrime is a particular facilitator of the close collaboration and cooperation between TGNs. As Walden has observed, the ease with which States can claim jurisdiction over cybercrime[228] means that "the foreign LEA can choose to investigate the alleged conduct without a formal request having been received, on the basis that the investigated conduct also constitutes an offence in their territory."[229] This was confirmed in my interviews with LEAs. SOCA interviewee (3) (**S3)** noted that their organisation often requested their counterparts in agencies like the FBI to conduct investigative actions on their behalf, which were said to be a much smoother and straightforward interaction when a criminal offence is also being committed in the US: "it's easier if there's some common ground, which very often there is for cyber[crime] because of the way it's structured."[230]

Many governments, including the UK, are specifically encouraging TGNs to cooperate in this way, and even to share information about their own citizens directly with foreign counterparts. The Home Office Guidelines for foreign LEAs,[231] for example, prompts these authorities to consider police-to-police liaison as an alternative for certain information, including when seeking "details of UK telephone subscribers and telecommunications data for **non-evidential purposes**."[232] Such information is often the crucial cog required to unlock a cybercrime investigation, and could mean foreign LEAs could build an entire case against UK based cybercriminals, without ever seeking formal assistance from the UK. The guidelines even envisage police-to-police requests for "information and intelligence concerning investigations into offences which have been committed in the UK."[233]

Moreover, as discussed in the introduction and the previous chapter, the Convention is promoting the work of these TGNs through a variety of means. Article 26 states that Parties can "forward to another Party information

---

20/12/2014). See also Urbas (2012), 9, on the way US LEAs have fostered close relationships with their Eastern European counterparts.
[228] See chapter five.
[229] Walden (2013), 56.
[230] SOCA Interviewee (3).
[231] Home Office, 'Requests for Mutual Legal Assistance in Criminal Matters: Guidelines for authorities outside of the United Kingdom' (11th ed, 2014), 41.
[232] Ibid. Original emphasis.
[233] Ibid.

obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party." More importantly, it requires the creation of a 24/7 network: a point of contact available 24 hours a day, seven days a week, which must assist other countries in the provision of technical advice, preservation of data, the collection of evidence, locating suspects, and the provision of legal information.[234] This idea builds on the G8 24/7 network, which contains an even greater number of countries than have ratified the Convention.[235] These network points are usually based within law enforcement agencies,[236] and sit on the border between formal assistance and informal assistance. They can be used to facilitate formal cooperation, but more often operate for the provision of information, or preservation of data,[237] and such informal relationships will usually not even be based on any defined policy between the interacting agencies.[238] While they are currently under-utilised in practice,[239] which could be explained by numerous factors,[240] there is clearly potential for further exploitation.

There are, however, numerous concerns with the operation of these networking LEAs and general concerns with TGNs are particularly pertinent in this context; they can be "opaque venues for the exercise of unfair and inequitable power"[241] where powerful States can coerce other actors to secure preferred outcomes,[242] ignoring globally optimal outcomes by prioritising domestic concerns.[243] As Bronitt argues:

---

[234] Article 35(1).
[235] Over 49 countries are members of this network: http://www.oas.org/juridico/english/cyb_pry_G8_network.pdf (Accessed 20/12/2014).
[236] UNODC Cybercrime Study (2013), 212.
[237] Ibid, 211.
[238] Ibid, 210.
[239] 'Assessment Report: Implementation of the Preservation Provisions of the Budapest Convention on Cybercrime' (T-CY, 8th Plenary, 5-6 December 2012), 78. (**Implementation Report**). Countries like the US, however, are known to be inundated with 24/7 requests. SOCA interviewee (3) said that the UK's 24/7 network was not greatly availed of, speculating that it was due to the lack of any significant Internet infrastructure being based in the UK.
[240] It could, for example, be a result of the current high levels of direct cooperation between LEAs (rather than going through domestic 24/7 points of contact first), the role of liaison officers, and the fact that many service providers work directly with the most active countries in cybercrime investigations.
[241] Newman and Zaring (2013), 255.
[242] Verdier (2009), 130.
[243] Ibid, 126.

> "there is a danger that transnational policing activity falls outside the domain of domestic or even international accountability, operating in a legal shadowland with only limited legal and normative guidance for those engaged in cross-border law enforcement."[244]

Hufnagel and McCartney, in a similar vein, argue that "both European and international policing networks are frequently established outside governance and accountability frameworks."[245] Nevertheless, the above has shown that States are increasingly entrusting these actors with alleviating the bottleneck channels of MLA, and the Convention is undoubtedly also playing a role in their promotion.

4.5 Conclusion

Lombois once eloquently captured the limitations of enforcement jurisdiction:

> The law may very well decide to cast its shadow beyond its borders; the judge may well have a voice so loud that, speaking in his house, his condemnations are heard outside; the reach of the police officer is only as long as his arm … he is constable only at home.[246]

This chapter demonstrates why this is no longer an accurate statement, as LEAs are being fitted with extendable arms, and are being assisted through laws such as the DRIP Act 2014 and judicial pronouncements such as the *Microsoft* decision. The former casts not a shadow, but a beaming light across the world, while the latter was not simply heard in Ireland, but felt there as well. While the traditional mechanisms of international cooperation, such as MLA, may be "ill-suited to an era in which offences can be, and are, committed from across the world in real time",[247] such powers are only one room of the constable's home. Operating through networking interactions with foreign service providers, domestic service providers (regardless of where the data is located), suspects' devices (again regardless of where the data is located, or even where the device is located on recent Dutch authority), or the flourishing and increasingly penetrative work of TGNs, we are seeing policing powers transcending borders. McLuhan's global village[248] has become a reality,

[244] Bronitt (2012), 281.
[245] Hufnagel and McCartney (2014), 118.
[246] Lombois (1979), 536, cited and translated in Trudel (1998), 1047.
[247] Choo, Smith, and McCusker (2007), 72.
[248] McLuhan (1962).

as recognised by both the Head of EC3[249] and La Forest J., [250] but it is not only the international criminal community which is circumventing borders, as La Forest J. presumed.[251]

Bellia states that "[t]here are strong arguments that the customary international law prohibition on performing law enforcement functions in the territory of another sovereign applies even when law enforcement officials do not [physically] enter the territory of another state."[252] The difficulty, as the above chapter has shown, is in determining when 'functions' are actually performed in another country. Investigations that are now performed routinely, such as setting up fake social networking sites and engaging with suspected child sexual offenders in foreign countries,[253] could be said to involve not only transnational enquiries,[254] but also the accessing of data in a foreign country without the consent of the target or of the State where the data is located. Many States would no doubt be of the view that an understanding of the concept of territoriality and the principle of non-intervention, which would preclude such activities or some of the activities discussed above (such as analysis of suspects' mobile phones when they are within the jurisdiction and have been served with a search warrant) would be impractical and overly restrictive. Writing at around the time of the invention of the World Wide Web, Damrosch pointed to "a rather serious gap between what a broad view of the nonintervention norm would require and what states actually do."[255] This gap appears to be increasing, but Damrosch's point was not that the principle had fallen into desuetude, but that its scope can be changed through customary practice, and that it can be problematic to read the norm too widely.

---

[249] https://www.europol.europa.eu/content/global-action-against-dark-markets-tor-network (Accessed 20/12/2014).
[250] *USA v Cotroni* [1989] 1 SCR 1469, 1485, *per* La Forest J.
[251] Ibid.
[252] Bellia (2001), 100.
[253] There are a number of reported cases involving such transnational activities. See e.g. the Australian case *R v Priest* [2011] ACTSC 18 (11 Feb 2011) and the UK prosecution of Julian Oliver, discussed in O'Floinn and Ormerod (2011). These cases also reveal the potency of the TGNs who work together once they have identified suspects.
[254] As mentioned in chapter two, section 2.2, LEA enquiries abroad are regarded as illegal by esteemed international law scholars such as Mann (1984), 223.
[255] Damrosch (1989), 2.

My purpose in this chapter has not been to attempt to delineate a normative interpretation of the concept of territoriality for cybercrime investigations, but to show how it is being transformed by State practice, with the Convention, and interpretations of it, also promoting expansive exercises of investigative powers. On standard textual analysis, the Convention contains provisions that already have far-reaching consequences (e.g. Article 18(1)(a)), but the Transborder Group and others are reading it to be even more revolutionary in the realm of enforcement jurisdiction (e.g. Article 32(b)). Should States ever accept certain aspects of the Transborder Group's Protocol, the concept of territoriality would cease to provide any coherent or meaningful restraint on the activities of cybercrime investigators.

Of course, in practice, a number of asymmetries still leave many States' LEAs relatively impotent in cybercrime investigations: geographical asymmetries (e.g. where the major service providers are located, which is often the US); political asymmetries (e.g. countries such as the UK having good relationships with foreign service providers), and capacity asymmetries (e.g. some countries being massively under-equipped to conduct cybercrime investigations.) One difficulty with the current paradigm is that if only a small cluster of countries can investigate, there is a greater incentive to assume all of the workload, and conflicts of criminal jurisdiction arise through the unilateral exercise of enforcement powers. Even if these are not direct disputes between prosecutors or investigators,[256] they can nevertheless become protracted battles for the States involved.[257] The harmonisation process, in theory,[258] ought to alleviate the concentration of enforcement power, as States empower their domestic authorities in investigating and prosecuting cybercrime. But given these asymmetries, this theory often does not translate into practice. Moreover, with the suppression process now clearly aimed primarily towards the expansion of procedural enforcement powers, when more States do begin to invest further in domestic policing capacities, the stage is set for jurisdictional concurrency to become an even greater problem than it is at present. A greater number of countries will have the powers to seize evidence, and to seek the arrest of

[256] See chapter six.
[257] See chapter seven.
[258] See chapter three and Kohl (2007), 220.

individuals through extradition, related to cybercrimes over which numerous countries could claim jurisdiction.

Kohl has said that the "[f]requent lack of enforcement jurisdiction in respect of online conduct has no doubt played a significant role in keeping a lid on the number of cases where States would otherwise have asserted jurisdiction."[259] In light of all of the above, this statement also requires re-evaluation. To explore the ramifications of these new and expansive enforcement powers, we must turn to another jurisdictional transformation, which is the second key facilitator of conflict: the substantive law on cybercrimes and the jurisdictional scope of these offences. The next chapter focuses particularly on how concepts of territoriality have been defined and interpreted in a country that has traditionally been seen to have one of the most restrictive approaches towards criminal jurisdiction: the UK. It shows how, in the context of all of the offences in the Convention, UK law allows for the most expansive of claims to territorial jurisdiction.

[259] Kohl (2007), 106.

Chapter 5: The Ambit of Cybercrime

> "The enormous expansion of federal criminal jurisdiction outside our Nation's boundaries has led one commentator to suggest that our country's three largest exports are "rock music, blue jeans, and United States law."[1]

5.1 Introduction

A variety of taxonomies for categorising and defining cybercrime exist,[2] with some accounts simply distinguishing between cyber-dependent crimes (offences only committed using computers and computer networks), and cyber-enabled crimes (conventional crimes that are facilitated and often rendered more effective with the advent of computing).[3] The Convention, however, divides cybercrimes into four categories: computer-integrity crime, computer–related crime, content-related crime, and criminal copyright infringement. I will broadly adopt this categorisation for present purposes (although like Walden,[4] will treat copyright infringement as a form of content offence), and this chapter is structured around the applicable offences in England and Wales (**E&W**)[5] for each category of offence.

The ultimate purpose of the chapter is to demonstrate the malleability of territorially focused criminal offences in the context of cybercrime, and the short-sightedness of transplanting jurisdictional provisions from other suppression conventions, into the Convention, without any mechanisms for dealing with jurisdictional concurrency beyond a nudge towards consultation. Working my way through the three main categories of offences in the Convention, as found in the criminal laws of England and Wales, I analyse the jurisdictional issues that have arisen in the case-law, or could arise given the wording of the offences. This analysis reveals that, although the criminal law of these countries is often considered too conservative towards accepting

---

[1] *United States v. Verdugo-Urquidez* (1990) 494 US 259, 280-1 *per* Brennan J, quoting Grundman (1980).
[2] See chapter one, note 1 and Walden (2007), 20-24.
[3] See McGuire and Dowling (2013).
[4] Walden (2007), 23.
[5] My focus is on the law of these countries, though for simplicity I will sometimes broadly refer to 'the UK', and I will not address the circumstances where there is overlap or divergences with the criminal law applied in Scotland or Northern Ireland.

jurisdiction over cross-frontier offences,[6] in the context of cybercrime the ambit of these offences is cast widely, and the ease with which an offence can be said to be committed within the 'territory', is startling. When even a Convention State with a traditionally conservative approach to jurisdiction embraces exercises that have a tenuous territorial connection, this highlights the potential for conflict and aggressive jurisdictional assertions by States.

5.2 Content Offences

I begin with content offences, being one of the most controversial areas of enforcement, and consider hate speech, child sexual abuse images and copyright offences. All have been facilitated considerably in the information age, raising complex jurisdictional questions, particularly given the transnational and organised nature of the offending in the latter cases.[7] Similar interpretative challenges have arisen in each category of content crime regarding the application of elements involving 'publication' or 'making available' over the Internet, and we will see the UK courts adopting far-reaching interpretations across the offences.

5.2.1. Content Offences 1: Hate Speech

One of the most controversial issues during the drafting of the Convention involved attempts to include provisions covering the distribution of racist and xenophobic material.[8] Due to the free speech orientations of countries such as the US, consensus could not be reached for the purposes of the Convention,[9] but a Protocol additional to the Convention was adopted in 2003, "concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems."[10] The offences that must be established pursuant to the Protocol are broadly defined and include: the dissemination of racist and

[6] Ryngaert (2009).
[7] See discussion of the complexity of cybercrime investigations in chapters four and six.
[8] See e.g. 'Racism and Xenophobia in Cyberspace', Motion for a Recommendation, Parliamentary Assembly, Council of Europe (7 November, 2000).
[9] Explanatory Report to the Cybercrime Convention, para. 35.
[10] Additional Protocol to the Convention on Cybercrime (CETS No: 189. 28 January 2003). The Protocol entered into force in 2006, and has been ratified by 22 countries, as of 20 December 2014.

xenophobic material[11] through computer systems (Article 3); racist and xenophobic motivated threats of criminal conduct (Article 4); racist and xenophobic motivated insults (Article 5); and denial, gross minimization, approval or justification of genocide or crimes against humanity (Article 6).

Free speech libertarians were expectedly critical of this initiative, but the Protocol has also been criticised for paying too much heed to freedom of expression[12] with the result that it is not fit for purpose.[13] Brennan, of the latter perspective, critiques the Protocol for vagueness in the definition of the offences, and for under-inclusion of other types of hatred, such as religious hatred.[14] She controversially asks why "race hate as opposed to hate more generally, is given priority."[15] This under-appreciates the elusive nature of 'hate speech' and the difficulty of defining the concept.[16] An equally formidable task lies in determining *where* the offences occur when they are committed over the Internet.

5.2.1.1 Hate Speech Offences in E&W

The UK is not a signatory to the Protocol,[17] but there are a range of offences in England and Wales that could be used to prosecute the hate speech offences contained therein. For example, the 'racially or religiously aggravated' offences contained in sections 31 and 32 of the Crime and Disorder Act 1998 will cover many of the circumstances envisaged by Articles 4 and 5 of the Protocol, and a number of 'threat' offences, such as section 1 of the Malicious

[11] Defined in Article 2(1).
[12] Harris, Rowbotham, and Stevenson (2009), 172.
[13] Brennan (2009).
[14] Ibid, 126.
[15] Ibid.
[16] For discussion of these difficulties see Harris, Rowbotham, and Stevenson (2009), 157.
[17] Previous statements from the government have not provided a convincing or coherent narrative for this inaction. It is said to be due to a belief that its laws for dealing with incitement to racial hatred are sufficient, and that ratification of the protocol would "not allow us to maintain our threshold for this sort of offence." See Hansard (written answers), vol 471, 29 January 2008, col 209W. It is not clear how ratification would have this effect, particularly given the reservation provisions inserted into the Protocol, which allow for the choice of not being bound by certain provisions, and the fact that UK law would already meet most of the criminalisation obligations in the Protocol. Moreover, other harmonisation initiatives are applicable, notably, the EU Framework Decision on Combatting Racism and Xenophobia (2008/913/JHA, 28 November 2008).

Communications Act 1988, could also be used, although not specifically targeted at racist and xenophobic communications.[18]

However, the offences which most directly cover the situations envisaged in Articles 3-6 of the Protocol are to be found in Part III of the Public Order Act 1986 (**POA 1986**). The most relevant offences, for present purposes, are those contained in sections 18, 19 and 21. The underling features of each of these offences is that a person does an act which is 'threatening, abusive or insulting' and 1) intends thereby to stir up racial hatred, or 2) having regard to all the circumstances racial hatred is likely to be stirred up thereby. These crimes then respectively involve using words or behaviour or displaying any written material (section 18), publishing or distributing written material (section 19), and distributing, showing or playing a recording of visual images or sounds (section 21). English law has even gone further than the Protocol in some ways, by criminalising inciting religious hatred,[19] and hatred on the grounds of sexual orientation.[20]

One of the reasons why these provisions currently have a broad scope is because they have been interpreted as conduct crimes, although this was not entirely clear given the history of the provisions. The drafters of sections 18 and 19 of the POA 1986 drew from both section 6 of the Race Relations Act 1965,[21] and section 5A of the Public Order Act 1936 (**POA 1936**).[22] These provisions had been interpreted by the courts as 'context-dependent' crimes,[23] a subset of result crimes coined by Jaconelli, which are usually found in speech offences.[24] Here the critical question in determining whether an offence occurred "will be the susceptibility of the person or persons to whom the words

[18] There is unfortunately little coherence across the range of 'threat' offences found in English law. See Alldridge (1994).
[19] Racial and Religious Hatred Act 2006.
[20] Section 74 of the Criminal Justice and Immigration Act 2008.
[21] This was subsequently amended and inserted into s.5A POA 1936, by s.70 Race Relations Act 1976.
[22] For an excellent discussion of the historical development of hate speech offences in the UK, see Rumney (2003).
[23] See in relation to s.5 POA 1936 Lord Parker in *Jordan v Burgoyne* [1932] 2 QB 744, 749. Hepple (1966), 314, argued that s.6 Race Relations Act 1965 was also context-dependent claiming "the speaker or publisher must take his audience as he finds them." Jaconelli (1995) relies on *obiter* comments in *R v Britton* (1967) 2 QB 51, to suggest that s.6 was also a context-dependent crime.
[24] Jaconelli (1995), 772.

or printed material in question have been spoken or published."[25] Drawing on the predecessors of the offences in the POA 1986, Jaconelli argued that it was far from clear that the offences in sections 18, 19, and 21 of the POA 1986 had been rendered context-independent.[26] He pointed in particular to the trio of adjectives "threatening, abusive or insulting", claiming it is unclear whether they would, or should, be interpreted in a context-dependent manner.[27]

The current approach of the courts is to apply an objective test to this trio of words, [28] and in cases involving Internet or web communications, other elements of the offences have also been interpreted broadly. Of most importance in this context is the interpretation of when an item is displayed, published or distributed within the jurisdiction. This was considered in *Sheppard,*[29] where two individuals were prosecuted for various charges of possessing, distributing, and publishing racially inflammatory material. A comic which cast doubt on the occurrence of the holocaust was uploaded by Sheppard to a website, operated by him, called heretical.com. The defence argued that no publication occurred in the jurisdiction because publication only occurs in the jurisdiction in which the content is stored and hosted[30] (in this case, California) and claimed in the alternative that publication required a 'publishee.'[31] Essentially, the defendants argued that in order to show there was a publication to the public or a section of the public, as required by section 19(3), it had to be established that members of the public actually viewed the publication. The only evidence in court of this occurring was the testimony of one police officer, who had accessed the website, but as a 'self-publishee', the defence contended, there was no publication for the purpose of section 19.[32]

The latter argument failed as it was said to be based on an irrelevant comparison with the law on libel;[33] the prosecution only needed to show "the

[25] Ibid.
[26] Ibid, 776.
[27] Ibid.
[28] Ormerod (2011), 1097, and *R v Sheppard and Whittle* [2010] 1 WLR 2779, [35]: "the offences of displaying, distributing or publishing racially inflammatory written material do not require proof that anybody actually read or heard the material."
[29] *R v Sheppard and Whittle* [2010] 1 WLR 2779.
[30] Ibid, [19].
[31] Ibid, [34].
[32] Ibid, [34].
[33] Ibid, [35].

material was generally accessible to all or available to or was placed before or offered to the public."[34] No proof was required that any person actually read or heard the material, and the evidence of one police officer was sufficient to demonstrate the general accessibility of the material. This aspect of the decision in *Sheppard* has won plaudits from commentators,[35] and it is consistent with interpretations of other content-related crimes that can be committed over the Internet.[36]

Neither was it accepted that publication could only occur where the material is hosted (a country-of-origin theory).[37] The 'substantial measure' test from *Smith*[38] was embraced, which allowed the Court to circumvent analysis of the various jurisdictional theories mentioned by the defence.[39] Utilising this tool, the case before the Court was straightforward, as all of the material acts related to the uploading occurred within the jurisdiction, and "[t]he only 'foreign' element was that the website was hosted by a server in Torrance, California."[40] The lack of engagement with the various territoriality theories was "regrettable",[41] but certainly not unexpected; had the Court prioritisatised one theory of territoriality (e.g. a country-of-origin approach) this would have circumscribed considerably the situations where the crime could be prosecuted

---

[34] Ibid, [34]. The prosecution of Christopher Philips for distribution of videos on social media sites was on similar grounds, in the context of s.21 POA 1986. See http://www.cps.gov.uk/news/latest_news/man_sentenced_for_stirring_up_racial_hatred/ (Accessed 20/12/2014),

[35] See e.g. Gillespie (2010), 208.

[36] Section 127 of the Communications Act 2003, for example, was treated as a conduct crime in *DPP v Collins* [2006] UKHL 40, [8] and [21], with criminal liability not dependent on whether the offensive communication was actually received by an individual, or whether the persons who receive it are offended by it. See, however, *DPP v Chambers* [2012] EWHC 2157, [32]: "The effect of the message on those who read it is not excluded from the consideration." The mainstay of academic authority also supports such an interpretation of section 1 of the Malicious Communications Act 1988 as a conduct crime. See e.g. Walden (2007), 152 and Ormerod (2011), 1081.

[37] It is, however, non-sensical to describe *Sheppard,* as Dyson (2010), 8 did, as a case where "a US server has made Englishmen liable for a crime in England." Englishmen made themselves liable when one of them uploaded to his website material which was illegal in this jurisdiction, from this jurisdiction.

[38] *Smith (Wallace Duncan) (No. 4)* [2004] QB 1418. See discussion in chapter two, section 2.4.

[39] These were the country-of-origin approach (where the material was hosted), the country-of-destination approach (where the material was downloaded), and the targeting theory (where the material was targeted).

[40] *R v Sheppard and Whittle* [2010] 1 WLR 2779, [32]. Indeed, the case could also have been determined straightforwardly under the terminatory theory, given the interpretation of s.19 as a conduct offence. As soon as Sheppard uploaded the material from within the jurisdiction, and it was accessible, the crime may have been completed.

[41] Dyson (2010), 8.

within the jurisdiction. However, the result of this lack of engagement is a number of potentially "far-reaching offence[s]"[42] as the 'substantial measure' test is a flexible tool which can be used to widen the ambit of hate speech offences with ease. It could be interpreted to embrace situations where the only domestic element involves the hosting of the material within the jurisdiction, or even where the only territorial connection is accessibility, particularly if there is some degree of targeting the UK public,[43] although what it means to target is "very much up for grabs."[44] Indeed, mere accessibility of content has been sufficient for prosecution and jurisdictional purposes in the context of other offences, which are discussed next.

5.2.2. Content Offences 2: Child Sexual Abuse Images

A 'content' crime that caused much less difficulty for the drafters of the Convention was Article 9. This sets out a range of criminal offences in relation to child sexual abuse images[45] including their production, distribution or transmission, procurement, possession, or the offering or making available of such material, through computer systems. While debates continue regarding issues such as the definition of a child for these purposes,[46] and the types of material prohibited,[47] there is near universal consensus across law enforcement communities concerning core categories of images capturing abuse involving very young children, and there is, as a result, active cooperation between LEAs

---

[42] Ormerod (2011), 1082.

[43] Although analysis of jurisdictional theories was avoided, Scott Baker LJ did stress that "[t]he material was aimed primarily at the British public." *R v Sheppard and Whittle* [2010] 1 WLR 2779, [32]. See further section 5.2.3 below, concerning copyright offences.

[44] Schultz (2008), 818. In the German decision of *Töben* [2001] 8 Neue Juristische Wochenschrift 624, for example, although the anti-Semitic material was uploaded in Australia, the court found jurisdiction on the basis of the objective territorial principle (it was accessible in Germany), and justified its decision on the basis of the nexus the material had with Germany's history. This reasoning is unpersuasive given that as Kohl (2007), 101 notes "the site [was] of universal interest and … the online publication was in English."

[45] Although the Convention uses the term 'child pornography' it has rightly been observed how "such language acts to legitimize images which are not pornography, rather, they are permanent records of children being sexually exploited and as such should be referred to as child sexual abuse images." See https://www.iwf.org.uk/about-iwf/remit-vision-and-mission (Accessed 20/12/2014).

[46] The Convention, in Article 9(3), prevents Parties from adopting a definition that is lower than 16 years of age.

[47] For example, whether computer generated images ought to be criminalised remains an issue of controversy. For general discussion see Clough (2010), 255-282 and Gillespie (2011), 150-176.

in this area.[48] The seriousness of these crimes, combined with the fact that consumption of such material is a prevalent and widespread problem in many countries,[49] can result in a strong desire to pursue foreign suspects involved in its creation and distribution.[50] In the UK context, we will see that there is little, from a criminal law perspective, to prevent pursuit of such foreign targets, particularly when the approach of the courts in this area is considered alongside the case-law pertaining to obscene publications. The latter is not a form of criminality addressed in the Convention, but is an area from which the courts are likely to draw when considering jurisdictional issues pertaining to child sexual abuse images. While there may not be sufficient consensus internationally for universal jurisdiction to apply to this criminality,[51] if other States replicate the approach of the UK courts in this area, *de facto* universal jurisdiction would basically exist.

5.2.2.1 Child Sexual Abuse Images in E&W

The offences referred to in Article 9 of the Convention are addressed by section 1 of the Protection of Children Act 1978 (**PCA 1978**) and section 160 of the Criminal Justice Act 1988 (**CJA 1988**). The latter criminalises possession of indecent photographs of children, while section 1 of the PCA 1978 creates a range of offences including, *inter alia*, the taking, making, distributing or showing of indecent photographs of a child.

Like Article 9 of the Convention, the elements of section 1 of the PCA 1978 are in the widest of terms with considerable overlap in the various forms that the offence can take.[52] This is done, *inter alia,* to ensure inbuilt fail-safes in the event that some elements are interpreted narrowly in light of technological

[48] See in particular the work of the Virtual Global Taskforce: http://www.virtualglobaltaskforce.com/ (Accessed 20/12/2014).
[49] For example, Operation Ore involved 6000 suspects in the United Kingdom alone. See http://news.bbc.co.uk/1/hi/uk/2652465.stm (Accessed 20/12/2014).
[50] In the *Regpay* case involving the redlagoon.com child pornography site, US LEAs lured Belarusian citizens to France and Spain for extradition, since Belarus did not have an extradition agreement with the United States. For discussion see Sansom (2009).
[51] Gillespie (2011), 305. Sufficient agreement could not even be reached regarding possession of child sexual abuse images in the Convention, as Parties can reserve the right not to criminalise this activity (Article 9(4)).
[52] In the context of Article 9, for example, it is not clear what distinction there is between distribution and transmission, or between offering and making available. The Explanatory Report to the Convention, para. 95 suggests that 'offering' means 'solicitation', but this is an atypical interpretation of the word.

developments. In the domestic context, the legislator seemingly did not need to exercise such caution. In *Bowden*,[53] for example, the downloading of child sexual abuse images for private consumption was held to constitute a 'making' of them. It was accepted that the images would not have existed within this jurisdiction unless downloaded by the perpetrator.[54] This reasoning has been followed in cases such as *R v Smith and Jayson* to include the downloading of email attachments, and even the automatic transfer of images to a temporary browser-cache following viewing.[55] These decisions raise numerous issues for criminal doctrine, including the legal categorisation of 'downloaders' as being equivalent to the actual producers of the material.[56]

Equally broad interpretations of the other elements of section 1 of the PCA 1978 may be expected should foreign suspects involved in child sexual abuse images come before the courts. Even if all of the material acts were committed abroad, if such content was made available to members of the public within the UK it could be found to constitute a 'showing' or 'distribution', and thus an offence within the jurisdiction.[57] Such a far-reaching approach has been taken in the context of the offence of obscene publication, contrary to section 2(1) of the Obscene Publications Act 1959 (**OPA 1959**). Space does not permit for a detailed elaboration of the elements or interpretations of this opaque offence,[58]

---

[53] *R v Bowden* [2001] QB 88.
[54] Ibid, 90.
[55] *R v Smith and Jayson* [2002] EWCA Crim 683, [33].
[56] Akdeniz (2008), 56 and Walden (2007), 145-6.
[57] 'Showing' has been accepted to require active conduct, but there has been little other interpretation of the word in this jurisdiction. See *R v Fellows and Arnold* [1997] 1 Cr App R 244, 255. Active conduct could simply constitute the facilitation of access to the material for members of the public in the UK, such as by making purchases available in pounds sterling, and communicating with individuals in the UK regarding access and providing passwords. The latter acts constituted 'active' conduct in *Fellows*, although the defendant in that case was within the jurisdiction when 'showing' the material by making it available for viewing online.
[58] The obscenity test was described by Lord Wilberforce as "a formula which cannot in practice be applied," *DPP v Whyte* [1972] AC 849, 862. It is defined in s.1 OPA 1959 and has been rendered even more problematic by its interpretation in *R v GS* [2012] EWCA Crim 398, which concerned an explicit conversation about paedophilic sex acts between GS and an unknown individual, over internet relay chat. Despite s.2(1) OPA 1959 clearly constituting a context-dependent crime, it was found that publication could occur to only one individual, and the obscenity test could be met even when "the identity of the recipient is not known." (*R v GS* [2012] EWCA Crim 398, [22]). Since the offence is paternalistically targeted at protecting likely readers/recipients from being depraved and corrupted, this interpretation is irreconcilable with the test in s.1 OPA 1959. It also fails to recognise that the publishee in *GS* may have been in a foreign country, such as the US, conversing in a manner that did not constitute an offence there. It is, nevertheless, illustrative of the broad approaches taken by the courts towards the elements of such cybercrimes.

but it will suffice to observe that 'publication' under the OPA 1959 includes distribution or showing or transmission of data stored electronically[59] (thus bearing commonalities with the elements of section 1 PCA 1978), and to note the implications of two decisions which interpreted publication in the context of obscenity involving the Internet. The decisions of the Court of Appeal in *Waddon*[60] and *Perrin*[61] found publication to have occurred both where there is a single download of 'obscene' material within the jurisdiction, or where the material is accessible within the jurisdiction even if uploaded abroad.

In both cases, the defendants admitted responsibility for the relevant publication, but there was a crucial difference between them: in *Waddon,* the uploading of the material occurred in this jurisdiction;[62] in *Perrin,* it appears to have been argued that the French citizen, resident in London, had performed all material acts outside of the jurisdiction.[63] There was, in any event, "no evidence as to where the data files were created and posted, and there was no evidence as to the location of the server."[64]

The Court of Appeal, in both cases, found there was publication within the jurisdiction on the basis of section 1(3)(b) of the OPA 1959, and the cases have been interpreted to mean 'publication' under the Act can occur in the place where the material is downloaded. This is at least an accurate statement of *Waddon,* but the *ratio* of neither case is quite so clear-cut. Hirst, for example, criticises the decision in *Perrin* and contends a major error occurred in the Court's reliance on *Waddon*. He argues that *Waddon* was based on the terminatory theory, because "the occurrence of a relevant transmission within the jurisdiction could not realistically be disputed"[65] and the preparation and uploading of the material occurred in England. The statement in *Waddon* that "there can be publication on a website abroad, when images are there

[59] Section 1(3) OPA 1959.
[60] *R v Waddon* [2000] All ER (D) 502.
[61] *R v Perrin [*2002] EWCA Crim 747.
[62] *R v Waddon* [2000] All ER (D) 502, [10].
[63] *R v Perrin* [2002] EWCA Crim 747, [4].
[64] Ibid, [33]
[65] Hirst (2003), 189.

uploaded; and there can be further publication when those images are downloaded elsewhere",[66] is therefore treated as mere *obiter*.

I argue that Hirst's interpretation of the *ratio* in *Waddon* is incorrect. In *Waddon,* the above statement, described as *obiter,* is in the context of a defence submission that the only publication occurred in the United States, rather than England.[67] The Court held that this submission was based on the false assumption that there could only be one publication.[68] It did not, however, dispute the submission that the initial publication occurred where the website was hosted, rather than where the material was actually uploaded from.[69] The *ratio* of the case was that publication occurred when the police officer downloaded the material in this jurisdiction.[70] In other words, it was not Waddon's uploading within the jurisdiction which was determinative of where the publication occurred.

On the other hand, the Court of Appeal in *Perrin* did not decide the offence occurred in England and Wales because a police officer had viewed the material there, even though this did occur, and the court did endorse the decision in *Waddon*.[71] The 'type' of publication relied on was not to a named individual; "[t]he publication relied on in this case is the making available of preview material to any viewer who may choose to access it."[72] Transmission of data in section 1(3)(b) can therefore occur anywhere in the world, and once the material is 'available' within the jurisdiction, the offence occurs there.

A further feature of *Perrin* is its rejection of a 'substantial measure' test for determining when offences are committed within the jurisdiction.[73] This may be in need of revision considering the developments in *Smith* and *Sheppard*, however, it simply highlights that on either approach towards territorial jurisdiction, the criminal law is far-reaching. The traditionally conservative

---

[66] *R v Waddon* [2000] All ER (D) 502, [12].
[67] Ibid, [8].
[68] Ibid, [12].
[69] This is clear from the court's description of the defence concession, when read with the statement that "there can be publication on a website abroad, when images are there uploaded." Ibid, [10]&[12].
[70] Ibid.
[71] *R v Perrin* [2002] EWCA Crim 747, [18].
[72] Ibid, [22].
[73] Ibid, [52].

terminatory theory was found to be sufficiently flexible to cover situations where the only domestic nexus was the accessibility of content, while the substantial measure test has been noted to be a malleable tool which could cover a similar situation, particularly if the UK public is targeted. Given the overlap in the elements involving child sexual abuse images, and the fact that this is a more serious category of criminality, it is highly likely that the courts would adopt a similar approach in the context of section 1 of the PCA 1978. Moreover, extraterritorial jurisdiction applies to these offences[74] when committed by nationals or residents (subject to double-criminality), and it even extends to individuals who were neither at the time of the offences, but have assumed residence or nationality at the time the proceedings were brought.[75] Therefore, both through the courts and the legislator, the ambit of domestic law pertaining to child sexual abuse images has expanded considerably in recent years, with foreign actors, or domestic actors disseminating this material abroad, readily found to be committing offences within E&W.

5.2.3. Content Offences 3: Copyright Offences

There is little need to recount the difficulties the content industries face with the advent of streaming sites and the variety of file-sharing mechanisms that have emerged in recent years. While criminal enforcement of Intellectual Property (**IP**) laws has long been recognised,[76] it has traditionally been left to rights-holders to protect their interests through civil laws, and a variety of mechanisms are currently being deployed in the UK, including volume litigation[77] and the blocking of websites by access providers.[78] Nevertheless some countries (notably the US) have gone to great lengths to secure criminal convictions for copyright infringement, including pursing foreign suspects through costly extradition procedures.[79] There have also been a number of criminal prosecutions in the UK. Like child sexual abuse images, the problem

[74] Sexual Offences Act 2003, s.72(10) and Schedule 2, para. 1d.
[75] Sexual Offences Act 2003, s.72(3)&(4).
[76] Walden (2007), 127.
[77] See Murray (2009).
[78] The first case to utilise s.97A of the Copyright, Designs, and Patents Act 1988 against access providers was *Twentieth Century Fox Film v BT* [2011] EWHC 1981, and such orders have now become commonplace.
[79] See discussion of the O' Dwyer, Dotcom, and Griffiths cases in chapter seven.

of copyright infringement is increasingly treated by States as being on an epidemic scale, and exacerbated by the Internet. Although still a costly, time-consuming process for rights-holders and police, it may well be expected that criminal cases will continue, particularly if current efforts to prevent infringement[80] do not have the required effect. Indeed, the Intellectual Property Office in the UK is currently considering raising penalties for online copyright infringement,[81] which evidences a continued desire to employ the criminal law for these purposes.

Article 10 of the Convention requires Parties to ensure criminal offences are available in respect of infringements of copyright[82] and related rights[83] where such acts are committed wilfully, on a commercial scale, and by means of a computer system. It does not purport to define the specific infringements that must be covered, referring to definitions in domestic laws implementing relevant international agreements, which only set down a minimum level of protection which State Parties must adopt.[84] Copyright's national character can no doubt lead to significant conflict between States where differences exist in the interpretation of laws,[85] but conflicts are also likely even where there is consensus on whether acts constitute infringement, particularly in our current information society. In this section I consider the ambit of English criminal law for such offences, and argue that developments in the civil sphere are suggestive of it having an increasingly broad scope when applied to acts in the networked environment.

[80] See e.g. the recent launch of 'Creative Content UK', by major access providers and rights-holder groups.
[81] For critique see the Open Rights Group response: https://www.openrightsgroup.org/ourwork/reports/response-to-survey-on-raising-maximum-penalty-for-breaching-online-copyright-to-10-years-in-prison (Accessed 20/12/2014).
[82] Article 10(1).
[83] Article 10(2).
[84] See e.g. the Berne Convention for the Protection of Literary and Artistic Works, 1886.
[85] See e.g. the domain name seizure of the 'roja directa' sports streaming site by the US, despite the legality of the site having passed judicial scrutiny in Spain: http://www.huffingtonpost.com/2011/02/02/rojadirecta-org-seized_n_817458.html (Accessed 20/12/2014).

5.2.3.1 Copyright Offences in E&W

The UK meets its Article 10 obligations with a range of statutory offences found in the Copyright, Designs and Patents Act 1988 (**CDPA**)[86] as well as through common law offences such as conspiracy to defraud. The most pertinent for the purposes of online copyright infringements are the offences found in section 107 of the CDPA, and it will be sufficient to focus on a handful of these to demonstrate the breadth of these offences.

Section 107 criminalises, *inter alia,* the distribution of an infringing copy of a copyrighted work,[87] or communicating a copyrighted work to the public,[88] in the course of business where the person knows or has reason to believe that what is involved constitutes copyright infringement. The same offences (distribution and communication to the public) can also be committed even otherwise than in the course of business, if the distribution is to such an extent as to affect prejudicially the owner of the copyright.[89]

The nature of modern file sharing technologies exposes vast swathes of the world to prosecution under these sections. Peer–to-peer file sharers using the BitTorrent protocol and BitTorrent clients such as uTorrent, for example, will normally both download as well as distribute or make available copies of copyrighted material (frequently films or music) and the case-law to date confirms that offences would be committed in these circumstances. In *Polydor*[90] a summary judgment was granted in respect of a user of Limewire, who (apparently unwittingly) made more than 400 audio files available to the public.[91] Similarly, in *Dramatico*, in the context of applications for injunctions against access providers under section 97A of the CDPA, Arnold J. found that users of The Pirate Bay make sound recordings available to the public within the meaning of section 20(2)(b) of the CDPA.[92] There is little doubt that such

[86] See e.g. ss.107, 198, 297, 297A, and 296ZB CDPA.
[87] Section 107)(1)(d)(iv).
[88] Section 107(2A)(a). Section 20(2) defines communication to the public, as including broadcasting a work, or making it available to the public by electronic transmission in such a way that members of the public may access it from a place and at a time individually chose by them.
[89] See s. 107(1)(e) and s. 107(2A)(b) respectively.
[90] *Polydor Ltd v Brown and others* [2005] EWHC 3191.
[91] Ibid, [8]-[9].
[92] *Dramatico Entertainment & Others v BSkyB & Others* [2012] EWHC 268, [69]-[70].

reasoning could also apply in the criminal context,[93] and successful convictions have been secured against file sharers for distributing infringing copies of copyrighted works, otherwise than in the course of business, contrary to section 107(1)(e).[94] In *Muir*,[95] for example, a woman made thousands of digital music files available to the public, which was sufficient to prejudicially affect the owner of the copyright, and would presumably come within the meaning of "on a commercial scale"[96] in Article 10 of the Convention. Since an average ITunes library contains over seven thousand music files on some estimates,[97] and with approximately 500 million unique IP addresses sharing files on peer-to-peer networks in the first six months of 2014 (with the UK in the top three countries for IP addresses involved),[98] the number of individuals who could potentially face prosecution is vast.

However, the operators of torrent indexing sites,[99] or streaming sites, are presumably the preferred targets of criminal prosecutions. While a case in the UK in 2010 suggested that convictions against the operators of such sites would be difficult to secure,[100] this jurisprudence has since been overtaken by developments in the civil courts. The CJEU has adopted a broad interpretation of the meaning of "communication to the public" in the context of Article 3 of

[93] The definition of communication to the public in s.20(2)(b) also applies to s.107(2A) CDPA.
[94] See e.g. the prosecutions of Phillip Danks: http://www.independent.co.uk/life-style/gadgets-and-tech/movie-pirate-given-almost-3-years-in-prison-for-filming-fast--furious-6-in-back-of-cinema-9686167.html (Accessed 20/12/2014) and Kane Robinson and Richard Graham http://www.bbc.co.uk/news/uk-england-tyne-29993498 (Accessed 20/12/2014).
[95] http://www.sln.law.ed.ac.uk/2011/05/10/first-illegal-music-file-sharing-conviction-in-scotland/ (Accessed 20/12/2014).
[96] The meaning of 'commercial scale' in other contexts continues to be a matter of dispute. See Adam (2011).
[97] Study by TidySongs, see http://mashable.com/2011/01/04/itunes-library/ (Accessed 20/12/2014).
[98] TruOptik, 'Digital Media, Unmonetized Demand, and Peer-to-Peer File Sharing' (2014), 11 & 31, available at: http://www.truoptik.com/reports (Accessed 20/12/2014).
[99] The operators of The Pirate Bay, for example, were convicted in Sweden for copyright offences. See *Sweden v Neij and others (*Case no. B13301-06, 17 April 2009).
[100] In *R v Rock and Overton* (Gloucester Crown Court, T20097013, 2010), charges of conspiracy to defraud and communication to the public contrary to s.107(2A) CDPA were dismissed in relation to the operators of a streaming site (tv-links.co.uk). Since the site did not host the content, it was found not to have made it available within the meaning of s.20(2). The *ratio* of the case, however, is difficult to discern due to reliance on the mere conduit defence found in reg.17 of the Electronic Commerce (EC Directive) Regulations 2002. In another case, *R v Ellis* (Middlesbrough Crown Court, T20087573, 2010), a jury failed to convict on a charge of conspiracy to defraud against the founder of a BitTorrent indexing site, Oink.

the Copyright Directive,[101] and the UK courts have held that such a communication occurs in the relation to the operation of Usenet websites,[102] streaming sites,[103] and torrent indexing sites.[104] This is despite the fact that none of the content is stored by the websites concerned. However, even if a narrower interpretation were taken towards the meaning of communication to the public, these website operators would undoubtedly be liable as accessories. The operators in all cases were also found to be joint tortfeasors, and accessorial liability in relation to IP offences is oddly one of the areas where the criminal law is less demanding than civil law.[105]

Therefore, a range of individuals could be liable for copyright offences in relation to streaming and file sharing websites. The criminal laws of numerous countries will invariably be engaged in this environment, which could include the countries where the uploaders or site owners are operating from, the countries where the content is stored (country of emission), or even where it is accessible. In relation to section 107(2A) of the CDPA, English criminal law will most clearly apply where the website operators or uploaders of content are located within the jurisdiction.[106] It may also apply, however, even where these individuals are based abroad, particularly if they have targeted the UK public. The CJEU has adopted targeting criteria in relation to a number of related rights, including distribution rights,[107] and database rights,[108] and this has been

[101] Copyright and Information Society Directive (2001/29/EC, 22 May 2001). This is usefully summarised by Arnold J. in *Paramount Home Entertainment & Others v BSkyB & Others* [2013] EWHC 3479, [12].
[102] *Twentieth Century Fox Film & Others v Newzbin* [2010] EWHC 608, [125].
[103] *Paramount Home Entertainment & Others v BskyB and Others* [2014] EWHC 937, [35]; *Paramount Home Entertainment & Others v BskyB and Others* [2013] EWHC 3479, [32]; and *FAPL v BskyB & Others* [2013] EWHC 2058, [42]. There is currently some uncertainty in relation to whether individuals who provide links to content which was not made available with permission from copyright holders, (*contra* the position in *Svensson* (Case C-466/12, 13 February 2014)), constitutes a communication to the public, but the decision of the CJEU in *BestWater* (Case C-348/13, 21 October 2014), relating to embedded videos, suggests that it may not. The issue should be addressed directly in the pending reference in *C More Entertainment v Sandberg* (C-279/13).
[104] *EMI and Others v BskyB and Others* [2013] EWHC 379, [45].
[105] For example, knowingly assisting a tort will not on its own constitute joint tortfeasorship, but knowingly assisting a crime would result in prosecution and punishment as if a principal offender, under s.8 of the Accessories and Abettors Act 1861. On this disparity, see Davies (2011).
[106] As occurred in the *Muir* case, *supra* note 95. See also the comments of Arnold J in *EMI Records and Others v BskyB and Others* [2013] EWHC 379, [41].
[107] *Donner* (Case C-5/11, 21 June 2012).
[108] *Football Dataco* (Case C-173/11, 18 October 2012).

interpreted domestically as also applying to acts of communication to the public. Arnold J. stated in *EMI* that "a communication to the public which originates outside the UK [but] is received inside the UK, … will be treated as occurring within the UK if the communication is targeted at the public in the UK."[109] The criteria that have been mentioned to determine targeting would suggest that this would not be overly difficult to establish in many cases,[110] and the near universal interest of some websites will mean that many States may be simultaneously targeted. For example, "websites streaming popular sports games … will attract a lot of visitors, regardless of the language of the commentaries."[111] Depreeuw and Hubin argue that in this situation "[w]here no specific public is targeted, the work is arguably made available [and communicated] to the public that has access to the work."[112] Therefore, the criminal copyright offences of the UK will be applicable to a range of foreign acts (whether the actors involved are based abroad, or the place of emission of the content), possibly on the basis of the mere accessibility of the content,[113] or at least where a malleable targeting criterion is satisfied. But this would not exclude the simultaneous applicability of other States' criminal laws, for example, the laws of the States from which the relevant actors were acting.[114]

Therefore, even if there currently does not appear to be a strong appetite within the UK for pursuing criminal convictions for copyright infringement against

[109] *EMI Records and Others v BskyB and Others* [2013] EWHC 379, [38].
[110] Factors that were mentioned in *Paramount* [2014] EWHC 937, [36], included the presence of advertisements in pounds sterling, or where the websites featured "recordings by UK artists which were … in demand in the UK."
[111] Depreeuw and Hubin (2014), 758.
[112] Ibid.
[113] In the context of Article 5 of the Brussels I Regulation (Regulation 44/2001 of 22 December 2000), the Court of Justice accepted a mere accessibility criterion in *Pinckney v Mediatech* (Case C-170/12, 3 October 2013), which involved the distribution of copyrighted music over a website. Doubt has been cast on this approach by Advocate General Cruz Villalón in *Pez Hejduk v EnergieAgentur.NRW* (Case C-441/13, 11 September 2014), suggesting that the delocalisation of damages over the Internet, means that Article 5(3) requires looking for the place where the "causal event took place" (translation of aspects of the decision by Eleonora Rosati, available at http://ipkitten.blogspot.co.uk/2014/09/breaking-ag-cruz-cruz-villalon-suggests.html (Accessed 20/12/2014)). This could be interpreted as the place where the content is uploaded from, or the place where it is stored. However, *Pinckney* remains authoritative in relation to Article 5 of Brussels Regulation I, and while neither case involves criminal law, interpretations of territoriality and harm in this context could easily be transposed to the criminal copyright offences.
[114] In *Football Dataco* (Case C-173/11, 18 October 2012), [47], it was recognised that infringements can take place both where the content is targeted, as well as other countries. This was also recognised by Arnold J. in *EMI Records and others v BskyB and others* [2013] EWHC 379, [41].

foreign operators, the above has shown that the ambit of English criminal offences provides broad scope for prosecution should such a course of conduct be chosen.

5.3 Computer-Related Offences

Chapter II(1) Title 2 of the Convention refers to "computer-related offences." While in name this category is hugely broad in scope, only "computer-related forgery" and "computer-related fraud" were actually targeted by the drafters. These are often inter-related offences (with the former often a pre-cursor for a fraud[115]) and there are myriad, constantly evolving ways of committing frauds online.[116] Quantification of the damage caused by these activities is notoriously difficult to determine, but police estimations of the cost of 'dating fraud'[117] in the UK alone, is in excess of £20 million a year.[118] The magnitude of the problem has resulted in a perception, in many quarters, that existing offences are insufficient and that new offences pertaining to 'identity theft' are required.[119] I have reservations as to whether further criminalisation is going to yield any significant results in terms of mitigating the damage caused by cyber frauds. The real problem in this area appears to be that the offences are almost invariably multi-jurisdictional in nature, which in turn creates enforcement challenges in locating and prosecuting those responsible.[120] However, this is an area to which law enforcement is paying particular attention,[121] with many

---

[115] http://www.bbc.co.uk/news/uk-england-18377246 (Accessed 20/12/2014).
[116] Examples include auction frauds or the numerous varieties such as advance-fee schemes. For further discussion see e.g. Clough (2010), 183-9, MacEwan (2013) and Chang (2008).
[117] This is a form of advance-fee fraud. For analysis of the modus operandi of these scams, see Whitty and Buchanan (2012).
[118] https://www.cityoflondon.police.uk/news-and-appeals/Pages/The-cost-of-online-dating-fraud.aspx (Accessed 20/12/2014).
[119] See e.g. Clough (2010), 190 and Recital 14 of the Directive on Attacks Against Information Systems (2013/40/EU, 12 August 2013), and the Centre for Strategy and Evaluation Services, 'Study for an Impact Assessment on a Proposal for a New Legal Framework on Identity Theft: Report for the European Commission', (2012). Countries such as Australia have enacted specific offences relating to, *inter alia,* dealing in identification information. See Australia Criminal Code Act 1995, division 370-2, as amended. In the UK, creation of such an offence would run contrary to existing authority that information cannot be stolen. See *Oxford v Moss* (1979) 68 Cr App Rep 183, and Walden (2007), 97 and 116.
[120] See e.g. the operations of any of the various cybercrime forums such as DarkMarket, Ghostmarket, or Confidential Access.
[121] See the work of 'Action Fraud' in the UK: http://www.actionfraud.police.uk/ (Accessed 20/12/2014). Two of EC3's three focal points (Cyborg and Terminal) are focused almost exclusively on fraud and related activities.

successful investigations and prosecutions being reported,[122] and involving close cooperation between networks of LEAs.[123] As with the other offences addressed in this chapter, when applicable offences are applied to the online world, analysis reveals a wide territorial ambit, which is significantly broader than has been recognised in the literature to date; foreign actors can commit fraud offences in the UK, even if no harm or loss occurs here.

5.3.1. Fraud Offences in E&W

The Convention focuses on the two forms of computer related offence: forgery and fraud. Discussion of the latter will suffice in demonstrating the jurisdictional scope of domestic fraud offences. Article 8 of the Cybercrime Convention recommends the adoption of a specific fraud offence defined by reference to modes of commission through the use of computers. The offence focuses on the intentional—and without right—causing of a loss of property to another person, with the added requirement of a fraudulent or dishonest intent of procuring an economic benefit for oneself or another. The conduct through which it is envisaged this will be done is through the manipulation of computer data,[124] or the interference with the functioning of a computer system.[125]

The fraud offence in Article 8 is relatively narrow in terms of the conduct it covers, since it is technology specific, and requires the causing of a loss of property. Ratifying States, however, may rely on existing criminal offences in order to implement the article,[126] and the UK can point to the Fraud Act 2006 (**FA 2006**) to this end. The FA 2006 abolished eight deception offences contained in the Thefts Acts 1968 and 1978, creating a general fraud offence in section 1 which can be committed through false representation (section 2), failing to disclose information (section 3) and abuse of position (section 4).

---

[122] In the UK, see e.g. the prosecutions of Renukanth Subramaniam (Darkmarket), Jason Place (Confidential Access), and Nicholas Webber (Ghost Market).
[123] See e.g. the recent prosecution of Maurice Asola-Fadola in Ghana: http://www.nationalcrimeagency.gov.uk/news/news-listings/478-romance-fraud-mastermind-jailed-in-ghana (Accessed 20/12/2014).
[124] Article 8(a) refers to 'any input, alteration, deletion or suppression of computer data.'
[125] Article 8(b). This is intended to include hardware manipulations. See Explanatory Report to the Cybercrime Convention, para. 86.
[126] Ibid, [80].

The previous law on deception was riddled with difficulties in proof, including the requirement to show that someone was actually deceived where 'someone' could not be a machine, as it was not possible in law for a machine to be deceived. This changed in section 1 with the law moving from result-oriented deception offences to conduct-based forms of fraud. Subsequent calls for a new e-fraud statute failed to appreciate that these changes removed the previous lacuna created by the impossibility of defrauding machines.[127] In fact, frauds utilising the Internet were specifically envisaged,[128] and section 2(5) of the FA 2006 extends the definition of 'representations' so as not to require a human recipient. Ormerod and Williams have even suggested that fraudulent statements, saved to a hard drive prior to being communicated, would be a representation caught by the FA 2006.[129] The new section 11 offence of obtaining services dishonestly is also specifically designed for cases where the obtaining was wholly by automated processes.

The broad ambit of domestic fraud offences can be demonstrated through analysis of the offence of fraud by false representation. Section 2 of the CJA 1993 provides that this offence will be committed within the jurisdiction when a "relevant event" occurred here,[130] with relevant event being defined as "any act or omission or other event … proof of which is required for conviction of the offence."[131] The FA 2006 expanded upon what constitutes a relevant event so as to include the occurrence within the jurisdiction of any gain or loss intended by the defendant.[132] Therefore, where a representation is made abroad, with intent to make a gain or loss within the jurisdiction, a charge for fraud by false representation will lie, "but only if there is an actual gain or loss within England and Wales."[133]

Ormerod is critical of limiting the interpretation of 'relevant events' so as to require proof of this result, given that the new offences are conduct crimes.[134]

---

[127] Hache and Ryder (2011), 49.
[128] See e.g. Explanatory Notes to the Fraud Act 2006, para. 16.
[129] Ormerod and Huw-Williams (2007), 145.
[130] S. 2(3).
[131] S. 2(1).
[132] Through insertion of s.2(1A) in the CJA 1993, by Schedule 1, para. 25 Fraud Act 2006.
[133] Ormerod (2007), 215. Original emphasis. See further Farrell, Yeo, and Ladenburg (2007), 95 and Ormerod and Huw-Williams (2007) 130-1.
[134] Ormerod (2007), 215.

However, section 2(1A) of the CJA 1993 merely *includes* the relevant events of gain or loss within the jurisdiction as sufficient for the ambit of the fraud offences with foreign elements. It does not tell us when, for example, a representation is actually *made* in this jurisdiction. Ormerod and Williams, in this regard, note the importance of the shift to a conduct-based crime in the FA 2006, meaning a 'representation' can be made before it is actually communicated to any person.[135] Further, a "representation may be articulated and communicated at different venues."[136] In other words, a representation can be made when sent, but may continue until it is received. This seems also to have been the Government's view when drafting the FA 2006. In its response to the Home Office consultation paper, it was noted how:

> no jurisdictional problem will arise in 'phishing' cases, even though the fraudster typically operates abroad. If he targets people in the UK by sending them false representations in order to obtain their personal financial details, with a view to making a gain or causing them loss, then he will be committing an offence of fraud which falls within our jurisdiction under the 1993 Act.[137]

Therefore, although the jurisdictional provisions in the CJA 1993 make it clear that where a person makes a representation to another person abroad, by word of mouth, an offence will only occur within England and Wales when there is intent and actual gain or loss within the jurisdiction, this result-oriented limitation will not apply to Internet frauds where people within the jurisdiction are targeted. American mail fraud law has been criticised because an email being routed through a server is sufficient for jurisdictional purposes,[138] but domestic law isn't far behind. The sending abroad of emails and accessibility of, for example, a fake banking website, is sufficient, and there is no need to prove actual gain or loss. But even without following this interpretation of the CJA 1993, many acts of cyber-fraud having an impact on the UK will involve some gain or loss within the jurisdiction, with section 2 of the FA 2006 clearly applying in that case, regardless of where the perpetrator is located at the time of communicating the false representation.

---

[135] Ormerod and Huw-Williams (2007), 140-3.
[136] Ibid, 147.
[137] Criminal Law Policy Unit 'Fraud Law Reform: Government Response to Consultation Paper' (2004), [54], available at: http://webarchive.nationalarchives.gov.uk/+/http://www.homeoffice.gov.uk/documents/cons-fraud-law-reform/Government_response.pdf?view=Binary (Accessed 20/12/2014).
[138] Home Affairs Committee 'The US-UK Extradition Treaty', Twentieth Report, (2012) 11.

I am under no illusions of the jurisdictional complexities of cyber-fraud investigations and prosecutions. As the SOCA once noted, "not all frauds are discovered, not all discovered frauds are reported and not all reported frauds are investigated."[139] But when investigations do occur, it is clear that the criminal law of E&W will not be a barrier to prosecution, regardless of where perpetrators are located when targeting UK victims.

5.4 Computer-Integrity Offences

Computer integrity offences (Articles 2-6 of the Convention) have been referred to as "true 'cybercrimes'"[140] in that without computers and computer networks, these offences would not exist. The offences contained in this section of the Convention broadly cover four different types of activity: access, interception, modification or interference, and misuse of devices. I have previously addressed some of the vagaries in the interception offences contained in RIPA,[141] and it will suffice for present purposes to focus on the domestic law relating to the basic illegal access offence in Article 2.

5.4.1. Computer Access Offences in E&W

Article 2 requires criminalisation of intentional and "without right" access to the whole or any part of a computer system. The corresponding offence in domestic law is found in section 1(1) of the Computer Misuse Act 1990 (**CMA 1990**),[142] and is committed where a person "causes a computer to perform any function with intent to secure access to any program or data held in any computer", the access he intends to secure is unauthorised, and he knows at the time when he causes the computer to perform the function that that is the case.

The concepts of 'access' and 'authorisation' are crucial for determining the scope of these offences. While the Convention has adopted a narrow 'box' approach towards the concept of access,[143] by evoking images of being inside

[139] SOCA 'The United Kingdom Threat Assessment of Organised Crime, (2009), 56.
[140] Clough (2010), 11.
[141] O'Floinn and Ormerod (2011).
[142] A more serious offence is found in s.2(1) which requires proof of an unauthorised access offence, as well as intent to commit or facilitate commission of further offences.
[143] See Articles 1(a) of the Convention.

or outside the computer,[144] a broader approach to access is found in the CMA 1990: the phrase "causes a computer to perform any function" would even cover switching on one's own computer, if it was to be used for accessing another computer with requisite intent. The concept of authorisation (or 'without right' in Article 1(1) of the Convention) is equally capable of broad interpretation,[145] and I have already addressed elsewhere the potential for expansive interpretations of the concept of authorisation in the CMA 1990,[146] with the attendant risks of overcriminalisation and "transform[ing] whole categories of otherwise innocuous behavior into … crimes simply because a computer is involved."[147] Within the EU, the most recent Directive on Attacks Against Information Systems has defined the basic access offence more narrowly than its predecessor,[148] by describing it as occurring where there is an infringement of a security measure,[149] which has long had support in the literature.[150] However, the CMA 1990 still defines authorisation widely in section 17(5), and it may even apply to the accessing of a webpage in breach of its terms of service.[151]

In this environment, the potential cross-border implications of activities were obvious to the drafters and detailed jurisdictional provisions were inserted. Section 4(1) provides, in relation to the section 1 offence, it is immaterial "(a) whether any act or other event proof of which is required for conviction of the offence occurred in the home country concerned; or (b) whether the accused was in the home country concerned at the time of any such act or event." In such cases, however, a "significant link" with domestic jurisdiction must exist,[152] which essentially arises where either the accused was in the home

[144] Clough (2010), 59. See also Clough (2011), 153. Kerr (2003), 1647-8 has demonstrated how this fails to account for the reality of computing in the networked environment.
[145] See for example, the differences that have emerged across different Appeal Circuits in the context of employee misuse of computer systems in the US: *US v Nosal* 676 F.3d 854 (9th Cir 2012) and *International Airport Centers LLC v Citrin* 440 F.3d 418 (7th Cir 2006).
[146] O'Floinn and Ormerod (2011), 772-3.
[147] *US v Nosal* 676 F.3d 854 (9th Cir 2012), 860.
[148] Article 2, Council Framework Decision on Attacks Against Information Systems (2005/222/JHA, 24 February 2005).
[149] Article 3, Directive on Attacks Against Information Systems (2013/40/EU, 12 August 2013).
[150] Kerr (2003), 1643.
[151] O'Floinn and Ormerod (2011), 772-3.
[152] Section 4(2) CMA 1990.

country[153] when he did the relevant act,[154] or that the computers containing the program or data to which he secured, or intended to secure, unauthorised access,[155] were in the home country concerned.

The scope of the offences therefore expressly embraces situations where, for example, X[156] types a command on his computer in an attempt to gain access to a computer abroad, or where Y abroad causes his computer to perform a function with intent to gain access to data in a computer within the jurisdiction. The offence in the latter situation is complete, in theory, as soon as Y turns on his own computer. The ambit of the section 2 offence (unauthorised access with intent to commit a further offence) is even broader. For example, there is no need to demonstrate a significant link with the home country,[157] provided the ulterior offence intended is triable in the home country. As Hirst points out, the "ulterior offence may even be an extraterritorial offence, in which case the section 2 offence requires no connection at all with England and Wales, and is itself fully extraterritorial."[158]

Moreover, despite the ease of claiming territorial jurisdiction over computer-integrity offences, the Directive on Attacks Against Information Systems has required that EU Member States adopt nationality jurisdiction over such offences, at least in situations where the act was an offence where it was committed.[159] As a result,[160] the UK is amending section 5 of the CMA 1990 to also include nationality jurisdiction (as a 'significant link') in relation to access offences.[161] This is further evidence of the myopic mind-set of governments and legislators, which views the expansion of jurisdictional bases as necessary in order to counter cybercrime.

---

[153] E.g. England and Wales, Scotland or Northern Ireland: s. 4(6) CMA 1990.
[154] Sections 5(2)(a) and 5(3)(a) CMA 1990.
[155] Section 5(2)(b) CMA 1990.
[156] See e.g. the McKinnon case, as discussed in chapter seven.
[157] Section 4(3) CMA 1990.
[158] Hirst (2003), 196.
[159] Article 12(1)(b) Directive on Attacks Against Information Systems 2013/40/EU (12 August 2013). Article 12(3) also envisages jurisdiction on the basis of residence, or where the crime committed was for the benefit of a legal person established in its territory, simply requiring that Member States inform the Commission if they enact provisions to this end.
[160] The UK has opted-in to this particular post-Lisbon criminal law measure: http://www.parliament.uk/business/news/2011/february/statement-on-eu-directive-on-attacks-against-information-systems/ (Accessed 20/12/2014).
[161] Section 42 Serious Crimes Bill.

5.5 Conclusion

The opening quote to this chapter noted the breadth of criminal jurisdiction in the US, a country known for aggressive jurisdictional seizures. However, the above has demonstrated that the domestic cybercrime laws permit equally broad jurisdictional assertions, and this was without even considering forms of inchoate liability. [162] The UK has been regarded as jurisdictionally conservative[163] but this requires reassessment, particularly as extraterritorial grounds of jurisdiction have also begun to be embraced; but it is in no way unique in having a broad ambit for its cybercrime laws. The UNODC Cybercrime Study asked participants whether their domestic law provided a sufficient framework for the "criminalization and prosecution of cybercrime acts committed outside of their country."[164] The study concluded that there is 'sufficient' jurisdiction: "forms of territoriality and nationality-based jurisdiction are almost always able to ensure that a 'sufficient connection' or 'genuine link' can be established between cybercrime acts and at least one state."[165] But the drafters of the Study do not fully appreciate the other side of the coin here, and the difficulties that can emerge from this panoramic approach to jurisdiction, which will be elaborated upon in subsequent chapters. In fact, they propose to develop model provisions on jurisdiction for a multilateral instrument, which would even include the effects doctrine.[166]

One of my central claims is that the malleability of the concept of territoriality,[167] and the ease with which States can claim territorial jurisdiction over a cybercrime, is a particularly insidious development. While it has long been recognised that tenuous assertions of *extraterritorial* jurisdiction can hamper international relations and cooperation, [168] it is the concept of

---

[162] See e.g. the US reliance on conspiracy charges in chapter seven. See also Hirst (2003), 134-182 and e.g. the abolition of the offence of incitement in the Serious Crimes Act 2007 through the creation of three new conduct offences (ss.44-46). The jurisdictional provisions for these offences have exceptional breadth. For example, D may be liable for acts capable of encouragement or assistance, regardless of where he was at the material time, "if he knows or believes that what he anticipates might take place wholly *or partly* in England or Wales" (s.52(1). Emphasis added.

[163] Ryngaert (2009).

[164] UNODC Cybercrime Study (2013), 190.

[165] Ibid, 196.

[166] Ibid, Key Findings and Options, p. xiv.

[167] See discussion in chapter two.

[168] Blakesley (2008), 1109. See also Ryngaert (2008), 188 and Gibney (1996).

territoriality over cyber-criminality that should be the greater concern. Territoriality is no longer a "straightjacket"[169] and a Kelsenian theory of interpretation assists to illuminate the reasons why this is so. This jurisdictional ground can be seen to be a norm "with a frame of possible meanings."[170] It is linguistically indeterminate, suffering from inherent vagueness due to a lack of precision as to the objects to which it refers.[171] For example, we have seen assertions of territorial jurisdiction on the basis of mere accessibility,[172] and exercising jurisdiction on the basis of the location of content is unquestioningly accepted by many States.[173] But with the norm cast so widely, "[a]ny act that stays within this margin and gives the frame a possible sense is legal."[174]

This has invariably resulted in highly questionable jurisdictional claims. In chapter seven, for example, we will see that the US often places considerable reliance on the location of servers involved in cybercrime in order to seek the extradition of foreign suspects. Interpreting territoriality in this way means that where a case is prosecuted can ultimately depend on the attractiveness of hosting providers' websites and costing models, and given the density of hosting servers in Western countries such as the US, will frequently facilitate their involvement in criminal prosecutions that may otherwise have little nexus with the country.[175]

As discussed in chapter two, international law does not provide any solutions here. The stalemate between the objective and subjective approaches to territorial jurisdiction has mapped directly onto the same debates in the cybercrime context,[176] and hierarchies between these forms of territoriality will

---

[169] Ryngaert (2008), 195.
[170] Kammerhofer (2011), 105.
[171] Ibid, 120.
[172] See further Kohl (2007), 96.
[173] In the area of hate speech, EU Member States are bound to ensure their territorial jurisdictional rules extend to information hosted in their territory: Article 9(2)(b) of the Framework Decision on Racism and Xenophobia (2008/913/JHA, 28 November 2008).
[174] Kelsen (1960), 348, translation by Kammerhofer (2011), 106.
[175] Basing jurisdiction on the location of servers may be more justifiable if prosecuting the hosting provider for failing to remove illicit material, with liability being premised on aiding and abetting the principal offence. However, even then, prosecution would seem more appropriate in the place where the hosting provider is located or established, which may not coincide with where the server is located.
[176] See for example, Kohl (2007), 25 on the equation of the country-of-origin and country-of-destination principles with subjective and objective territoriality. Both Kohl (2007), 90, footnote 84 and Parrish (2012), 9 also equate objective territoriality with the 'terminatory

not find favour with States. An exclusive objective territoriality/country-of-destination approach, defined either through an 'effects' or 'constituent elements' test, has the advantage of States retaining control over activities affecting their territories, but invariably leads to the problem of concurrent jurisdiction. The effects test, in particular, has been heavily critiqued for sanctioning exercises of jurisdiction on tenuous grounds, but in the context of cybercrime, these tests are almost indistinguishable.[177] When accessibility of a website can constitute the *actus reus* of an offence (e.g. 'making available' or 'publication'), the constituent elements approach is equally as broad a ground of jurisdiction as when focusing on the 'effects' caused by virtue of that accessibility. Conflicts may arise even where harmonisation has occurred,[178] as with the cybercrime offences addressed in this chapter, but are more likely where it hasn't.[179]

The alternative—a blunt prioritisation of the subjective territorial principle[180]—is equally impractical and unforeseeable. A first problem is that it is unclear what the 'subject' of the country-of-origin/subjective approach actually is in the context of cybercrime. It seems to be assumed in some of the literature, for example, that where an activity originates, where a website operator is based, and where the information on the website is hosted, will all coincide in terms of locality.[181] The reality of course, is that an Irish citizen could upload content in France, use a server in the US, a domain-name provider in Australia, and operate the site from England. Kohl's statement that "there is generally only

---

theory' found in English law. As discussed in chapter two, Hirst, Ryngaert and Goode have convincingly explained that these are distinct concepts.

[177] Hayashi (2007), 77.

[178] As the International Bar Association notes, "[e]ven when laws are harmonised, different legal systems are still likely to interpret the same rules in different ways." IBA, 'Report of the Task Force on Extraterritorial Jurisdiction' (2009), 31.

[179] In the context of content-offences, for example, a country-of-destination approach has the effect of publishers having to comply with the laws of all states, "and the most restrictive law in the world – the 'slowest ship' – would thus be able to set the tone." Schultz (2008), 813.

[180] As discussed in chapter two, this refers to where a crime was initiated or commenced and a prioritisation of this ground has been suggested by Williams (1965). Although Kohl does describe, at one point, the country-of-origin/subjective approach, as "the location of the source of the activity" (Kohl (2007), 24) it would be a misreading of her work to describe this as the place where the server, hosting the content, is located. She clearly understood the place where the activity originated to mean the place where the person responsible for the acts was located: Kohl (2007), 106.

[181] Kohl (2007), 164.

one country in which an activity originates"[182] assumes a simplicity that is often not present in the online context. Even if it were to be proposed to prioritise the place where the actor was located at the time of the offence, as was done by the drafters of the Stanford Draft Convention on Cyber Crime,[183] this would remain objectionable, as it would require States to forego prosecutions even in cases where they have been directly targeted.[184]

While there have been some attempts at navigating a middle ground,[185] which has strong support in the literature,[186] targeting and other such concepts are inherently malleable and are not going to be a panacea for the problems which I argue are arising from jurisdictional concurrency. Even a 'substantial measure' test retains considerable scope for broad interpretation and can well be expected to be interpreted by judges so as to 'pull for the home crowd', particularly in circumstances where domestic law enforcement has invested resources in the prosecution. As Kohl notes, the temptation of 'might-over-right' is frequently too great: "[w]hen in possession of enforcement power, States tend to exercise adjudicative jurisdiction ... upon the most tenuous basis."[187]

---

[182] Ibid, 25.
[183] Article 5(4) of the Stanford Proposal for an International Convention on Cyber Crime (2000). This was an academic report, prepared by a number of academics including Abraham Sofaer and Seymour Goodman. See http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm (Accessed 20/12/2014).
[184] See e.g. the *McKinnon* case, as discussed in chapter seven, section 7.2.
[185] See for example, the UK's 'substantial measure' test.
[186] Akehurst (1972-3) contends that the constituent elements approach should be abandoned in favour of locating jurisdiction where the 'primary effects' are felt, while Oehler (1983), 212, and Schultz (2008), 817-8, propose targeting theories, as they are seen to reduce the number of overlapping jurisdictions, enhance foreseeability of sanction, and provide for a more reasonable exercise of jurisdiction. Hirst (2003), 342, recommends a combination of almost all of the above: a constituent elements approach, where at least one element occurs within the jurisdiction which establishes a 'real and substantial link', and an effects jurisdiction where the constituent elements occur outwith the jurisdiction, but the effects are direct, substantial and intentional.
[187] Kohl (2007), 109.

Chapter 6: Addressing Jurisdictional Conflicts: Investigatory and Prosecutorial Negotiations

"Cybercrime cases are at our doorsteps. They're coming."[1]

"We are at the very beginning of all of this."[2]

6.1 Introduction

The previous chapter demonstrated the breadth of territorial jurisdiction as applied to cybercrime. However, it is widely said that this breadth does not generate the sorts of jurisdictional clashes that might be expected as a result. Scassa and Currie observe that "[s]imply because a state notionally has jurisdiction does not necessarily mean that it will have any interest in exercising it,"[3] while Schultz contends that "[t]he submission of Internet actors to a worldwide range of paper rules may be true, but their submission to effective rules is far more limited."[4] Indeed, Ram, a lawyer for the Canadian Department of Justice, delivered a paper in 2011 with one section titled "the non-problem of concurrent or overlapping jurisdiction,"[5] a perspective which has undoubtedly also been behind suppression projects such as the Cybercrime Convention. The preparatory works for the Convention against Transnational Organized Crime, for example, points out that:

> [c]oncurrent jurisdiction might not be a negative development, as it would indicate the interest of numerous States to deal with specific problems. In addition, conflicts of jurisdiction *were rather rare* and were invariably resolved at the practical level by an eventual determination of which jurisdiction would be ultimately exercised on the basis of the chances for successful prosecution and adjudication of the particular case.[6]

---

[1] Eurojust Interview.
[2] EC3 Interview.
[3] Scassa and Currie (2011), 1026.
[4] Schultz (2008), 813.
[5] Ram (2011), 26.
[6] Report of the meeting of the Inter-Sessional Open-Ended Intergovernmental Group of Experts on the Elaboration of a Possible Comprehensive International Convention against Transnational Organized Crime (Warsaw, 2-6 February 1998), UN Doc. C/CN.15/1998/5. Emphasis added.

Ram elaborates on why, even in an era of cybercrime, jurisdictional concurrency continues to be treated as a 'non-problem':

> [i]n general, and increasingly in the era of globalization, scenarios such as mass-frauds and cybercrime do raise competing jurisdictional interests, but the understandable desire of States where victims reside and serious effects are felt to take a leading role in prosecution and punishment is often tempered by the costs and complexities of conducting a multinational prosecution and of incarcerating the offender, especially over long periods, if he or she is convicted.[7]

Therefore, while any number of countries could seek to prosecute cybercrimes, issues of cost, capacity, and complexity act as a deterrent, and if one country actually bucks the trend and attempts to investigate and prosecute a multi-national cybercrime, States are said to be generally only too happy for this to occur, even if they also have a strong connection with the case, or their nationals are involved.

I do not doubt these current practical realities. It is fair to say that cybercrime is a significant threat,[8] but prosecutions rare. However, I do take issue with referring to concurrency as a 'non-problem.' In fact I have such concerns with this attitude that my remaining chapters will be dedicated to illustrating how concurrency *is* problematic, and how these problems have been exacerbated by cybercrime. In jurisdictional terminology, Ram's point can be re-characterised as treating negative conflicts of jurisdiction to be so prevalent as to render positive conflicts, or "conflicts of exercise of jurisdiction",[9] hardly worth worrying about. Negative conflicts are 'statutory' conflicts of jurisdiction,[10] which arise whenever there is concurrent criminal jurisdiction over acts, with none of the relevant countries exercising their potential enforcement power.

---

[7] Ram (2011), 27.

[8] The UK's most recent National Security Strategy categorized cybercrime as a Tier One Threat to national security, alongside international terrorism. *Threats* from cybercrime must, however, be distinguished from actual *harm*. For example, phishing campaigns usually have low response rates; a recent study by Google of a range Google/Gmail phishing sites found 13.7% of visitors to the fake sites submitted information.
See < http://conferences2.sigcomm.org/imc/2014/papers/p347.pdf> (Accessed 20/12/2014). There is, in other words, a distinction between technical victimisation, and actual harm. For more on the various forms of cybercrime threats, and on the disparity between cybercrime's high threat categorisation, and low levels of prosecutions,
see <http://theconversation.com/high-risk-cyber-crime-is-really-a-mixed-bag-of-threats-34091> (Accessed 20/12/2014).

[9] Herrnfeld (2013).

[10] Ibid, 185.

The expansion of jurisdictional grounds mitigates this threat, as it provides more countries with the capability to seize the initiative. The paradox of the current paradigm, however, is that when the problem of negative conflicts is placed on a pedestal, it paves the way for unprincipled extensions of jurisdiction, in the name of efficiency and enforcement, which in turn actually augments the threat of positive conflicts of jurisdiction.

This brief chapter introduces my problematisation of jurisdictional concurrency. It will consider how jurisdictional conflicts have been dealt with in harmonisation initiatives, both via transnational conventions as well as within the EU, and will then discuss a number of interviews which I conducted with prosecutors and investigators, both in the UK, and at Europol and Eurojust. My intent in conducting these interviews was to establish how, and whether, concurrent jurisdiction is causing practical difficulties for such entities in cybercrime investigations and prosecutions. This will provide the practical platform for exploring in my final two chapters two areas which I contend have been complicated considerably by the advent of cybercrime: extradition practices and the law pertaining *ne bis in idem*. Many of my concerns relate to pre-existing problems in international law. Concurrency has always raised the prospect of international disputefs and a breakdown in international relations; finding the most appropriate forum for prosecution, from a normative perspective, has always required a balancing of practicalities such as location of evidence; States have often struggled to appease foreign counterparts with domestic prosecutions; and defendants have long faced the threat of multiple prosecutions in different States from their actions. But I argue that the way States have traditionally dealt with jurisdictional concurrency, and purport to do so in the context of cybercrime, makes for a cocktail of dysfunctional flexibility of an entirely new order.

6.2 Resolving Conflicts in International Law

In the battle between avoiding overlapping jurisdictional laws, and ensuring there are no jurisdictional gaps that could result in impunity, States have erred on the side of caution and preference the latter objective. The jurisdictional provisions make this abundantly clear in both transnational crime conventions

and harmonisation initiatives within the EU.[11] As discussed in chapter three, Article 22 of the Cybercrime Convention, for example, requires States to implement jurisdiction on territorial grounds, and prompts[12] States to also introduce nationality jurisdiction, which as mentioned in chapter two, was not traditionally exercised for many crimes in the common law, and is jurisprudentially questionable. Provisions are also frequently inserted to ensure that other forms of seizure of jurisdiction are not excluded, provided it is not in breach of international law (the breadth of which has been described in chapter two).[13]

Obviously, the drafters of these instruments realise the consequence of this unmediated broadening of jurisdictional grounds, but either treat it as a non-issue, as discussed above, or decide to obviate the issue. As the commentary to another one of these conventions states:

> [t]he text does not attempt to deal with the well-known problem of deciding in which State an offence, elements of which are located in more than one State, should be deemed to have been committed. It will be for each national legal system to determine whether what occurred on its territory satisfies the definition of the relevant offence created by its own law.[14]

Harmonisation initiatives normally do not even create a hierarchy of jurisdictional grounds to assist cases of conflict,[15] despite it being widely accepted that territorial jurisdiction has primacy over other extraterritorial

[11] See e.g. Article 12(1)(b) Directive on Attacks Against Information Systems 2013/40/EU (12 August 2013). Article 12(3) also envisages jurisdiction on the basis of residence, or where the crime committed was for the benefit of a legal person established in its territory.
[12] Article 22(2) allows States to enter a reservation to this jurisdictional ground.
[13] See e.g. Article 22(5) of the Cybercrime Convention.
[14] Commentary on the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna, 20 December 1988) 1998 E/CN,7/590, para. 4.7.
[15] One exception here was Article 10(4) Framework Decision on Attacks Against Information Systems (2005/222/JHA, 24 February 2005) which provided that States, in the case of conflict, *may* take sequential account of the following factors: territoriality, nationality of the offender, and the place where the perpetrator is found. This provision was not kept, however, when the Framework Decision was repealed by the Directive on Attacks Against Information Systems 2013/40/EU (12 August 2013). Another Convention that does attempt to order jurisdictional bases is the League of Arab States Convention on Combating Information Technology Offences (Cairo, 21 December 2010). Article 30(3) states "[i]f more than one State Party claims to have jurisdiction over an offence set forth in this Convention, priority shall be accorded to the request of the State whose *security or interests* were disrupted by the offence, followed by the State in whose territory the offence was committed, and then by the State of which the wanted person is a national." This hierarchy is undoubtedly not going to be very helpful to resolve cases of jurisdictional concurrency, as the question of when a State's interests are affected is even more uncertain and vague than territoriality.

bases.[16] The drafters resign themselves to the fact that resolving conflicts arising from concurrency is too intractable a task. This apathy is partly justified on the grounds that "there is no adequate solution to this matter in the corpus of existing norms of customary international law."[17]

Therefore, the usual recourse in conventions is simply to nudge states towards consultation. Article 22(5) of the Cybercrime Convention, for example, states that "[w]hen more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution."[18] Use of the word "shall" is suggestive of this being a binding requirement, but the subsequent words make clear that this is not the case: consultation must only take place "where appropriate." The Explanatory Report to the Convention gives examples of when this might not be necessary, such as where "a Party is of the view that the consultation may impair its investigation or proceeding, it may delay or decline consultation."[19] This effectively renders the provision toothless: a Party that knows another country is interested in its case will already consult of its own initiative, if it wishes to do so, or will not if it envisages domestic complications.

Outside of EU structures and institutions (discussed below), there is therefore little assistance to be found in international law as to how concurrent jurisdiction ought to be negotiated in cases of conflicts of exercise.[20] There is, however, at least one bilateral agreement, which was agreed between the

[16] See e.g. Ryngaert (2008), 218 and Bassiouni (2014), 378. Of course, in the context of cybercrime, even stating that territorial jurisdiction will have priority will normally do little to alleviate concurrency, given the ease with which different States can claim a territorial connection.
[17] Commentary to 1988 Drugs Trafficking Convention, *supra* note 14, para. 4.4.
[18] A similar provision can be found in Article 15(5) of the UN Convention Against Transnational Organized Crime (2004).
[19] Explanatory Report to the Cybercrime Convention, para. 239.
[20] Status of Forces Agreements also deal with the allocation of jurisdiction, with provisions varying, but they often accord host nations with primary jurisdiction over crimes committed in their territories, with exceptions existing where e.g. crimes are committed between the personnel of the sending State, or where the actor was acting in an official capacity when the crime was committed. See http://www.globalsecurity.org/military/facility/sofa.htm (Accessed 20/12/2014). Consular conventions can also deal with criminal jurisdiction. See e.g. *Wildenhus' Case* 120 US 1 (1887).

Attorney Generals of the UK and the US.[21] This agreement—the UK/US Agreement— promotes a system of early contact between the two countries in cases of concurrency between them. Prosecutors and investigators are urged to "consult closely together from the outset of investigations",[22] although only "in the most serious, sensitive or complex cases where issues of concurrent jurisdiction arise." [23] When prosecutors cannot reach agreement after consultation, the offices of their Attorney Generals or Lord Advocate should take the lead on the resolution of the matter.[24]

The historical record suggests the UK/US Agreement has been of little use. The most obvious reason for this is because it "does not address the issue of where cases should be better prosecuted, and is silent on any formula for resolving competing prosecutorial claims."[25] Indeed, it resigns itself to stating how "[e]ach case is unique and should be considered on its own facts and merits."[26] Therefore, calling it a "prosecutor's deal" which "takes care of prosecutorial concerns but shows little regard for the interests of defendants"[27] seems to even exaggerate the extent to which it assists prosecutors. As the next chapter demonstrates, the UK/US Agreement did little to increase the likelihood of consultation, or of domestic consideration of prosecution,[28] even in cases where the US is seeking the extradition of a British national on much weaker jurisdictional grounds than could be exercised by the UK.

However, developments in the cybercrime sphere, which will be analysed in chapter seven, have generated attempts within the UK to address jurisdictional concurrency more directly with, *inter alia*, domestic guidance developed for

---

[21] 'Guidance for Handling Criminal Cases with Concurrent Jurisdiction Between the United Kingdom and the United States' (**the UK/US Agreement**). Agreed by Attorney General Lord Goldsmith, and Attorney General Alberto Gonzales, (18 January 2007).
[22] Ibid, para. 5.
[23] Ibid.
[24] Ibid, para. 4.
[25] Binning and Campbell (2008).
[26] The UK/US Agreement, *supra* note 21, [3].
[27] Brookson-Morris (2007), 600.
[28] The cases discussed in chapter seven make clear that the UK/US Agreement is not engaged, and the DPP is under no obligation to consider it, unless there has been a domestic criminal investigation in the UK. This is reinforced in the text of the Agreement itself, which explicitly provides that it "does not create any rights on the part of a third party to object to or otherwise seek review of a decision by UK or US authorities." US/UK Guidance, *supra* note 21, [13].

prosecutors handling concurrency cases.[29] The CPS Guidance substantially replicates guidance found in Eurojust, and as the EU is the "laboratory for the development of other cross-border forms of cooperation",[30] my next section considers how jurisdictional concurrency has been addressed in this region.

6.3 Resolving Conflicts of Jurisdiction in EU Law

Since the establishment of an area of Freedom, Security and Justice under the Treaty of Amsterdam, the EU has had a keen interest in the "prevent[ion] and settle[ment] [of] conflicts of jurisdiction between Member States."[31] A Green Paper on Conflicts of Jurisdiction[32] was published in 2005, with discussions on-going for years before any legislative instrument was proposed. Eventually, on the initiative of five Member States, a Proposal was published in 2009,[33] with chapter four of the proposal dedicated to the question of how to determine the "best placed jurisdiction" when an offence is committed within the jurisdiction of two or more Member States. In terms of criteria to determine this question it was suggested that there should be a:

> general presumption in favour of conducting criminal proceedings at the jurisdiction of the Member State where most of the criminality has occurred which shall be the place where most of the *factual conduct* performed by the persons involved occurs.[34]

The latter explanatory clause in the sentence obviously does little to assist in determining how to ascertain where 'most of the criminality has occurred.' It would fail even to assist in prioritising a jurisdictional base in the classic textbook example: where an individual shoots a gun across a border, hitting someone in the second territory. Invariably, this aspect of the Proposal fell

---

[29] CPS 'Director's Guidance on the Handling of Cases where the Jurisdiction to Prosecute is Shared with Prosecuting Authorities Overseas' (17 July 2013) (**CPS Guidance**). The UNODC Cybercrime Study (2013), 195 (discussed in chapter four), reported that none of the responding countries dealt with conflicts of jurisdiction in cybercrime cases through legislation.

[30] Boister (2012), 165.

[31] Article 31 Treaty on European Union, now Article 82(1)(b) Treaty on the Functioning of the European Union (Consolidated version at OJ C326, 26 October 2012).

[32] European Commission, 'Green Paper on Conflicts of Jurisdiction and the Principle of ne bis in idem in Criminal Proceedings' (COM 696 final, Brussels, 23.12.2005).

[33] Proposal for a Council Framework Decision on Prevention and Settlement of Conflicts of Jurisdiction in Criminal Proceedings (Council Doc. 5208/09 JF/NC/kr, 20 January 2009). Available at: http://register.consilium.europa.eu/pdf/en/09/st05/st05208.en09.pdf (Accessed 20/12/2014).

[34] Ibid, Article 15(1). Emphasis added.

apart upon scrutiny in the Council. The end product,[35] agreed only ten months after the Proposal, was a drastically different instrument, which becomes apparent even from reading the respective titles; it went from being a Framework Decision on prevention and settlement *of conflicts* of jurisdiction in criminal proceedings, to a Framework Decision on prevention and settlement *of conflicts of exercise* of jurisdiction in criminal proceedings. No longer did it attempt to determine the best placed jurisdiction; the objective of the Framework Decision became more concerned with preventing parallel criminal proceedings on the same facts, which could infringe the principle of *ne bis in idem*.[36] And no longer did the requirement to enter into direct consultations require seeking the "best placed jurisdiction";[37] the obligation to consult, which arises only when it is *established* that parallel criminal proceedings exist in two or more Member States, has the less ambitious aim of trying "to reach consensus on any effective solution." [38] The final Framework Decision, therefore, no longer contains any criteria for determining a best placed jurisdiction,[39] and the obligation to initiate contact with another Member State only arises if a competent authority has "reasonable grounds to believe that parallel proceedings are being conducted in another Member State."[40] There is no obligation to contact another Member State even if prosecuting an individual on tenuous jurisdictional grounds, and another State is manifestly the more suitable forum.

The end result is an instrument of dubious value, and it is not clear that it has actually altered practices within the EU in any meaningful way. The consultation requirement is in more absolute terms than is found in Article 22(5) of the Cybercrime Convention, but within the EU Article 54 of the Convention Implementing the Schengen Agreement (discussed in detail in chapter eight) already serves as a motivating force for a State, at the pre-trial or

[35] Council Framework Decision on Prevention and Settlement of Conflicts of Exercise of Jurisdiction in Criminal Proceedings (2009/948/JHA, 30 November 2009).
[36] Ibid, Recital 3, and Article 1(2)(b).
[37] Article 12(1) of the Proposal.
[38] Article 10(1) of the Framework Decision 2009/948/JHA.
[39] It simply refers to the Eurojust Guidelines, discussed below. Ibid, Recital 9.
[40] Ibid, Article 5(1).

trial stages of criminal proceedings,[41] to contact other Member States if it has reasonable grounds to believe criminal proceedings are already being conducted there. Otherwise, it risks its investigative and prosecutorial efforts being rendered nugatory by the courts.

A final reason to doubt the utility of the 2009 Framework Decision is because Eurojust was at this point already fully functional, and a process was well underway to enhance its operational effectiveness. As discussed in chapter three, Eurojust was set up with the objectives, *inter alia,* of stimulating and improving coordination of investigations and prosecutions in cases of serious crime concerning two or more Member States.[42] It is now an independent body of the EU, which acts as a facilitator and mediator between Member States. It can do this either through its national members (each Member State seconds a judge, prosecutor or police officer of equivalent competence), or through the College of Eurojust (which consists of the 28 National Members). Acting in either capacity, it can ask a Member State to "undertake an investigation or prosecution of specific acts",[43] or accept that one Member State "may be in a better position to undertake an investigation or to prosecute specific acts",[44] or to "coordinate between the competent authorities of the Member States concerned." [45] These formal settlement procedures, however, are rarely utilised.[46] Since its inception through to 2013, there have been only three recommendations where the College has asked a Member State to accept that one jurisdiction is better placed to undertake an investigation or prosecution,[47] and recommendations under Article 6 (where Eurojust acts through its National members) are also rare,[48] with non-binding opinions from the College pursuant to Article 7(2) (where National Members cannot agree on a conflict of

[41] "Parallel proceedings" are defined only as the pre-trial and trial stages of criminal proceedings in the instrument.
[42] Article 3 Consolidated Eurojust Decision, *supra* chapter three, note 35.
[43] Ibid, Article 6(1)(a)(i), Article 7(1)(a)(i).
[44] Ibid, Article 6(1)(a)(ii), Article 7(1)(a)(ii).
[45] Ibid, Article 6(1)(a)(iii), Article 7(1)(a)(iii).
[46] As Deboyser (2013), 107 notes "[i]ssues related to the choice of jurisdiction are normally and frequently resolved with the assistance of Eurojust as a facilitator and mediator, and formal recommendations are rarely needed."
[47] Ibid, 104.
[48] In 2012, only nine formal recommendations were made. See Eurojust Annual Report 2012, 18.

jurisdiction) even rarer.[49] Usually, cases of conflict are "resolved by way of informal recommendations"[50] after coordination meetings with the interested parties.[51]

The necessity for the consultation obligations imposed in the 2009 Framework Decision on conflicts of exercise of jurisdiction is even more questionable because Article 13(7)(a) of the revised Eurojust Decision creates a new obligation on Member States to inform their national member of "cases where conflicts of jurisdiction have arisen or are likely to arise."[52] A literal interpretation of this phrase would appear to even embrace statutory conflicts, but it has been suggested that it applies only to cases of conflicts of *exercise* of jurisdiction. As Herrnfeld notes:

> [i]t would go too far to interpret the provision as requiring the national authorities to inform Eurojust of every case where there is a possibility that one or more other Member State(s) may—in accordance with their law—also have jurisdiction over a certain case.[53]

Eurojust has also had more success in development of criteria for deciding which jurisdiction should prosecute in cases of concurrency. At a seminar in 2003, it developed a set of guidelines for these purposes,[54] which suggests that where a number of countries "*could* each institute proceedings in their own courts, there should be a meeting between nominated senior prosecutors representing each jurisdiction involved to discuss and agree where the prosecution should be mounted."[55] They contain a "preliminary presumption that, if possible, a prosecution should take place in the jurisdiction where the majority of the criminality occurred or where the majority of the loss was

---

[49] Deboyser (2013), 105 and Herrnfeld (2013), 188.
[50] Deboyser (2013), 105.
[51] Europol can also request a Member State to initiate a criminal investigation: Europol Decision (2009/371/JHA, 6 April 2009), Article 7. However, EC3 Interviewee (1) stressed that it would have to be an extraordinary case for a Member State to be formally requested to investigate, and that EC3's role is a more sensitive and subtle process. Rather than directly requesting, they usually simply bring the relevant countries together, provide the analysis of how the particular criminal enterprise is operating, and facilitate the conversation between the relevant investigating authorities.
[52] Consolidated Eurojust Decision, *supra* chapter three, note 35.
[53] Herrnfeld (2013), 187.
[54] 'Guidelines for Deciding Which Jurisdiction Should Prosecute', Published as an Annex to the 2003 Eurojust Annual Report (**the Eurojust Guidelines**).
[55] Ibid, 2. Emphasis added.

sustained."[56] It then provides a non-hierarchical list of factors that should be further considered in any decision, including the location of the accused, the capacity of a State to seek the extradition or surrender of the person, the centralisation of cases where possible, the attendance (and protection) of witnesses, evidential concerns, possible delays in prosecutions in particular jurisdictions delay, and the interest of victims. Factors that should not influence decisions include choosing a jurisdiction in order to avoid legal obligations in another, seeking to prosecute where penalties are highest, and the capacity of a particular country to prosecute should only be considered when all other factors are equally balanced. With such a diversity of criteria it is difficult to imagine a scenario where all other factors could ever be 'equally balanced.' However, in the cybercrime context, we will see that *capacity* to investigate and prosecute plays a much bigger role in such decisions than the drafters of the Eurojust Guidelines would like.

Upon reading these guidelines, one may be left with the impression of frequent and structured dialogues in cases of concurrency. This is particularly the case when one sees their impact in jurisdictions as far a field as Trinidad and Tobago,[57] and because, as mentioned, they have been almost directly transposed in the recent CPS Guidance. In practice, however, the Eurojust guidelines, at least directly, seem to assume less importance than might be thought. Moreover, their suggestion that every prosecuting authority *should* consult, whenever they *could* exercise jurisdiction, is even more (unrealistically) ambitious than Article 13(7)(a) of the Eurojust Decision; in the context of cybercrime, most Member States *could* exercise jurisdiction, but no prosecuting authority would have the manpower to engage in negotiations in each and every case. The Eurojust Guidelines also might give the impression that prosecutors have near exclusive competence in the negotiation of concurrent jurisdiction, but as the next section makes clear, this is not the case.

[56] Ibid, 3.
[57] *Steve Ferguson, Ishwar Galbaransingh v The Attorney General of Trinidad and Tobago* (CV 2010-04144, 7 November 2011), [73].

6.4 Negotiating Concurrency

As explained in my introduction, I conducted a number of 'purposive' interviews in my research,[58] and one of the issues which I explored was how jurisdictional concurrency was experienced amongst TGNs. By interviewing key investigators and prosecutors at the national level and within Europol and Eurojust, I was able to triangulate my findings and learn of the processes at a variety of levels of relevance.

The need to interview both investigators and prosecutors was apparent from an early stage in my research. While prosecutors are increasingly steering jurisdictional negotiations,[59] decisions made at the investigative stage can obviously have a direct impact on where prosecutions ultimately occur.[60] Coordination meetings at Europol's EC3, for example, can dictate how a particular criminal enterprise is to be investigated, and ultimately prosecuted.[61]

I mentioned in my opening gambit that some of the literature suggests that the current situation, in the investigation and prosecution of cybercrime, involves 'negative conflicts' being the norm, with 'positive conflicts' of exercise being a non-issue. This was most certainly the view of all of my interviewees as well. EC3 Interviewee (1) (**E1**) stated "quite honestly, there aren't that many fights [e.g. between investigators as to where to prosecute]."[62] SOCA interviewee (1) (**S1**) succinctly captured the primary reasons for this, which reiterates Ram's point in my introduction:

---

[58] See *supra* 1.4.

[59] SOCA interviewee (3) suggested that while historically decisions as to where prosecutions should occur were made by police in the UK, this is no longer the case. Although the CPS has not been directly granted powers to conduct jurisdictional negotiations under its establishing statute (The Prosecution of Offences Act 1985), prosecutors have assumed this role. It was noted how prosecutors are now frequently involved from the outset of SOCA's investigations, even travelling with investigators to review material: "it's mostly gone from a police to police issue, to a lawyer to lawyer issue."

[60] This is also recognised in the CPS Guidance: "[i]n practice in cross-border cases, issues of forum will usually be decided between the police of the two (or more) jurisdictions, often before prosecutors become involved." See http://www.cps.gov.uk/legal/h_to_k/jurisdiction/ (Accessed 20/12/2014).

[61] SOCA interviewee (2) noted, however, how prosecutorial involvement can be required from an early stage if dealing with particular countries, such as civil law jurisdictions with investigating magistrates.

[62] SOCA interviewee (2) also stated "there have been very few cases which I've come across where there has been a battle about where you should prosecute somebody."

> [y]ou can imagine from the outside maybe that if you don't have territorial jurisdiction really well defined, then it's going to lead to international disputes. The assumption there is almost that there'll be more than one State wanting to prosecute. But in fact, the opposite is true. There are not enough resources to go around. These are incredibly difficult prosecutions most of the time. You're lucky if anyone is in a position to prosecute.[63]

However, my interviews also revealed more subtle reasons for the present situation. One contributory factor has been that the EU entities one may expect to be actively involved in coordinating cybercrime investigations and prosecutions actually have little experience in dealing with either. E1 admitted that Europol "came into the play rather late when it comes to supporting cybercrime investigations"[64] and estimated that this only began in 2009. The figures from Eurojust are startling: in 2013, only 29 cybercrime cases were registered with Eurojust.[65] Given that the total number of cases registered in the same period was 1576,[66] this represents less than 1.8% of its workload.[67] As my Eurojust Interviewee (**EJ)** noted, "cybercrime is simply not a big part of our daily work." [68] This is not to say that cybercrime investigations and prosecutions have not been occurring; as the next chapter establishes, some countries, such as the US, have been incredibly active in prosecuting cybercriminals, even when they are based abroad. But any prosecutorial negotiations occurring in this context (if they occur at all), seem only to be between the investigating State and the State where the suspect is located; the wider net of potentially interested countries play no role.

Other factors inhibiting more coordination of prosecutions are the disincentives to conducting "altruistic investigations." [69] These can concern either investigations which are directly conducted for other countries, or where material is produced from domestic investigations, which could be shared with

---

[63] SOCA Interviewee (1). These factors were also mentioned in other interviews. My Eurojust Interviewee, for example, spoke of the 'amoeba-like' structures of those behind many phishing sites, with the members involved changing frequently depending on the countries being targeted, and the specific malware required.
[64] EC3 Interview.
[65] Eurojust Annual Review, 2013, 35.
[66] Ibid, 58.
[67] My Eurojust Interviewee did admit that there may be some problems with these figures in terms of how National Members classified the case. For example, an Internet fraud should be cited as both a fraud case, as well as a cybercrime case, but may not be labelled in the latter category.
[68] Eurojust Interview.
[69] SOCA Interviewee (3).

foreign counterparts. In *McKinnon*,[70] for example, much of the investigative work was conducted by the UK's (then) National High Tech Crime Unit, at the request of the US. The tension arises due to the ways of assessing the work of LEAs domestically. Effectiveness is often measured by factors such as the number of cases sent to domestic prosecuting authorities, with funding for the particular police authority directly linked to such statistics. EJ suggested that this often deters the sharing of the fruits of investigative work with foreign counterparts, and/or encourages States to pursue prosecutions domestically, even if it requires the costly extradition or surrendering of foreign suspects. This confirms my concerns with Ryngaert's theory of jurisdiction,[71] as networking actors struggle to pursue global interests, given domestic constraints.[72]

On the other hand, when States do get together to discuss cases of conflict, EJ stressed that the primary reason why "[t]he positive conflict is never a conflict [is] because everyone is happy to prosecute their own part."[73] This was also confirmed in a separate interview: "police tend to be very parochial. They like a local investigation and prosecution."[74] And this was cited as a primary concern in one of Eurojust's Annual Reports:

> [f]rom its casework, Eurojust has noted that in cybercrime cases, often multilateral by their very nature, negative conflicts have occurred: national authorities concentrate only on criminal activity within their boundaries rather than seeking to combat the problem at EU level.[75]

Therefore, in the (rare) situations where countries do get together at forums such as Eurojust, EJ suggests it is uncommon to find one country being dogmatic in attempting to assume the entire prosecutorial workload: "there's no conflict because usually they agree that 'we will prosecute our own nationals, our own victims, [and] this part of the case.'" The motivation for such an approach is relatively clear: it is cheaper to pursue, easier to manage, and less complicated. But it is said not to be an effective means of countering many forms of cybercrime activities. According to EJ, the near exclusive focus

[70] See the extensive discussion of this case in chapter seven.
[71] See further discussion in chapter two, section 2.6.2.
[72] Verdier (2009), 126.
[73] Eurojust Interview.
[74] SOCA Interviewee (1)
[75] Eurojust Annual Report 2010, 45.

on domestic harm is preventing the investigation and prosecution of the wider consequences, and of holding individuals responsible for the full extent of their criminality. It is also said to be preventing the apprehension of those behind these cybercrime groups.

There are, however, indications that this current paradigm is in the process of some transition. The very creation of EC3, and of Interpol's Digital Crime Centre in Singapore, should improve the intelligence and information base around these transnational cybercrime networks, thus improving the prospects of coordinating investigative activities. E1 noted that in the six months since the creation of EC3, he saw a significant increase in the amount of data being communicated to Europol by Member States concerning cybercrime,[76] as well as a greater volume of requests for coordination.[77] E2 also noted that Europol was actively pursuing further operational agreements[78] with countries that are seen to be crucial partners in the coordination of cybercrime investigations.[79] The figures from Eurojust are also revealing. The number of registered cybercrime cases in 2012 represented an almost 100% increase from the previous year,[80] while coordination meetings doubled between 2012 and 2013, and the number of Joint Investigation Teams increased from two to nine.[81] As EJ stated that "[t]he curve [of Eurojust's involvement with cybercrime cases] is growing, it's rocketing straight up, [and] I think it will automatically lead to cases of conflict."[82]

Concerns were expressed in my interviews at EC3 and Eurojust about their respective capacities[83] to cope with the volume of incoming data about cybercrime, and the legal challenges of coordinating cybercrime investigations,

---

[76] He estimated that there was an increase of approximately 60% from the same period in 2012.
[77] EC3 Interview.
[78] Article 23 Europol Decision (2009/371/JHA, 6 April 2009) allows Europol to establish operational and strategic agreements with third States and organisations. Operational agreements can include the exchange of personal data and classified information.
[79] Europol currently has operational agreements with twelve non-EU countries, and strategic agreements with six: https://www.europol.europa.eu/content/page/external-cooperation-31 (Accessed 20/12/2014).
[80] Eurojust Annual Review (2012), 29.
[81] Eurojust Annual Review (2013), 35.
[82] Eurojust Interview.
[83] As of June 2013, EC3 had only sixty-six members of staff, which includes those in supportive and administrative functions (confirmed over email exchange with EC3 Interviewee (3)). However, there are plans for further growth in 2014, according to EC3 Interviewee (1).

given that third States would invariably be implicated. While non-EU countries can and do participate in coordination meetings, EU data protection rules require operational or cooperation agreements prior to any sharing of personal data,[84] and only a limited number have thus far been agreed.[85]

However, even between EU countries the practicalities of conducting coordination meetings were said to be daunting. In Eurojust, the vast majority of coordination meetings have hitherto been bilateral in nature,[86] and EJ noted the practical difficulty of coordination meetings involving cybercrime, since they are "multi multi lateral."[87] E1 similarly mentioned the difficulty of operating Joint Investigations Teams, and coordination meetings at a police level, when even five or six countries were involved. The cases which Eurojust and Europol have dealt with, however, reveal that five or six countries is even below average in the context of cybercrime. Operation Rescue, an investigation of a child sexual abuse website, involved coordination between 14 countries, and resulted in 4,000 intelligence reports being sent to LEAs in 30 countries.[88] Operation Icarus, a similar case involving a child sexual abuse file-sharing networks, consisted of a coordination operation involving 23 countries.[89]

The limited coordination activities of Eurojust in the cybercrime realm reveal equal levels of complexity. Its Cases Analysis Unit was able to provide me with information in relation to three of the five coordination meetings held in 2012. One concerned a social network website used for the distribution of child sexual abuse images, and involved fourteen Member States,[90] as well as Europol and Interpol. The second involved an investigation in Austria into a malware distribution group, with the Austrian prosecutor requesting a

[84] See e.g. Council Framework Decision on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters (2008/977/JHA, 27 November 2008) and Article 28 of the Rules of Procedure on the Processing and Protection of Personal Data at Eurojust (2005/C68/01). For commentary see Belfiore (2013).
[85] Eurojust only has eight agreements with third countries: http://eurojust.europa.eu/about/legal-framework/Pages/eurojust-legal-framework.aspx (Accessed 20/12/2014).
[86] Eurojust interview. The point is confirmed, by Deboyser (2013), 106.
[87] Eurojust interview.
[88] Europol Review, 2011, 45. Nearly 800 suspects were identified in this case.
[89] Ibid, 46.
[90] Belgium, Czech Republic, Germany, Estonia, Spain, France, Ireland, Italy, the Netherlands, Norway, Portugal, Sweden, the UK, and the US.

coordination meeting with eight other Member States.[91] The third case involved an attack against an EU Registry, and involved thirteen countries.[92] As EJ mentioned, this is a relatively novel situation for Eurojust: "[e]ven with drug trafficking cases, usually there are only a couple of Member States involved—two or three. With cybercrime, it could be all of them, and [more] with third countries included… [These are] very complicated meetings."[93]

Given this complexity, one may expect that the Eurojust Guidelines would be at the heart of such meetings, but neither EJ, nor any of the EC3 interviewees, could ever recall these Guidelines being directly referred to in their respective coordination meetings. They were, however, unanimous in their belief that an exhaustive list of hierarchical factors could not function, and that guidelines such as those produced by Eurojust were all that were possible. As E1 noted, "I think the criteria in our area are not completely set, and cannot be … We look to things like who has the best information position, and who wants to prosecute."[94] This was the opinion voiced domestically as well. S2 said "the reality is it's likely to be a pragmatic conversation about where we are likely to have most success, and what that success looks like."[95] On the relevant criteria for determining who should prosecute, S1 suggested that "the starting point is often that prosecutions should be the jurisdiction of the suspect. But all kinds of practical and humanitarian reasons might dictate otherwise."[96] In another interview, it was also stressed how the value of criteria must be contextual, and in some cases, one could become a "knockout blow."[97] Examples given were cases where hundreds of documents may be in Greek, which would require translation, or the country where the suspect is located not extraditing its

[91] Belgium, Germany, Spain, Finland, Italy, the Netherlands, Norway, and the UK. Europol was also involved in the meeting.
[92] Austria, Belgium, Germany, Estonia, Greece, France, Hungary, Italy, Liechtenstein, Poland, Romania, Slovakia, and the UK. Europol was also involved in the meeting.
[93] Eurojust interview.
[94] EC3 Interview.
[95] SOCA interviewee (2).
[96] SOCA interviewee (1). SOCA interviewee (2) also mentioned practicalities such as evidence gathering; if the country where the suspect is located does not follow procedures which would allow for the admissibility of evidence in the UK, a foreign prosecution may be preferred, unless the UK was prepared to invest in the sending of investigators to that jurisdiction for evidence gathering purposes.
[97] Eurojust Interview.

nationals.[98] As the next chapter demonstrates, however, when variables such as those mentioned by E1 determine which country ultimately prosecutes an individual, the stage is set for positive conflicts of exercise to become the increasingly troublesome phenomenon that EJ predicted.

6.5 Conclusion

This chapter has traced the limited means through which suppression and harmonisation projects have dealt with jurisdictional concurrency, which usually only prompt consultations. It has also investigated the practical realities of these consultations when they do occur. It was found that amongst TGNs, positive conflicts and arguments concerning jurisdictional concurrency involving cybercrime were said to be rare. This was partially explained by the cost and complexity of cybercrime investigations, which also accounts for the relative infrequency of negotiations reaching supranational bodies such as Europol and Eurojust. These factors may lend support to the view that despite the breadth of territorial jurisdiction over cybercrime, "the job of everyone is the job of no one."[99] In other words, the fact that nearly every cybercrime is transnational can lead to inertia, with LEAs hoping their counterparts abroad will take up the helm.

However, conflicting forces were also identified. Factors such as domestic police funding can operate to incentivise unilateral pursuit of cases, and inhibit the coordination of investigations. The next chapter further demonstrates how the deterrent value of prosecuting transnational cybercrimes, through seeking the extradition of foreign suspects, can also be a powerful incentive for circumventing direct prosecutorial negotiations. The complexities of coordinating 'multi multi lateral' cybercrime investigations can also prompt States to 'go it alone.'

Moreover, one of my core arguments in this thesis is that while the "costs and complexities" [100] of cybercrime investigations may currently be dis-incentivising many State LEAs from pursuing cases against foreign suspects,

[98] Ibid.
[99] Klip (2012), 200.
[100] Ram (2011), 27.

this will change. It will change because of the inroads that are being made in terms of investigative powers, as discussed in chapter four. And it will change as more States begin capacity building and investing in cybercrime policing.

Therefore, there are interim problems, such as the resolution of jurisdictional concurrency becoming heavily dependent on factors such as who 'has the best information position', which will invariably be policing hegemons like the US, while ill-equipped TGNs will only too happily externalise the cost of the law enforcement. But there are long term concerns as it may soon no longer be an "unhappy marriage"[101] between the expansive breadth of criminal (territorial) jurisdiction and the frequent lack of enforcement jurisdiction; greater problems may arise with the marriage between breadth of criminal jurisdiction and *expansive* enforcement jurisdiction.

E1 noted that States must change their mind-set in cybercrime policing:

> [w]ith cybercrime, you cannot just say, 'cybercrime is committed in my country, so let's do an investigation.' It's an international problem, and you're part of it, and you need to figure out how to bring those parts together and agree on how to proceed.[102]

As the next chapter demonstrates, however, this mind-set is yet to be adopted by some, and we will see that in this disaggregated state system of transgovernmental cooperation there is a distinct danger of jurisdictional normativity being lost, with little space for its consideration within formal inter-State mechanisms. 'Bringing these parts together' has never been more difficult, and "we are at the very beginning of all of this."[103]

[101] Kohl (2007), 106.
[102] EC3 Interview.
[103] Ibid.

Chapter 7: Cybercrime Extraditions

> "There is a philosophy change. If you are going to attack Americans, we are going to hold you accountable. If we can reach out and touch you, we are going to reach out and touch you."[1]

7.1 Introduction

The previous chapter investigated, *inter alia,* how forum can be negotiated within TGNs. This chapter considers the procedural mechanisms for the movement of defendants between countries where such negotiations occur (and even where they don't, as we shall be seen). Extradition treaties and arrangements are constructs of some antiquity, dating from at least the 1200s BC.[2] For the majority of time since then, extradition was primarily used to prosecute political offenders, with common crimes either not enumerated, or not pursued. As Magnuson observes, however, by the 19th century "the situation flip-flopped."[3] Common crimes became the bread-and-butter of extradition requests, while political crimes were excluded. Oppenheim traced this development to the industrial revolution, where new technologies facilitated ease of transport between countries: "the conviction was forced upon the States of [civilized] humanity that it was in their common interest to surrender ordinary criminals regularly to each other."[4] The industrial revolution, therefore, not only changed the way that States perceived crimes,[5] but also changed the way extradition operated between countries. I argue that new technologies are having an equally profound effect today, as the Internet is facilitating ease of circumvention of punishment, just as railways and long-distance steamships did in the 19th century.

In one of the most influential pieces of literature on criminal justice, *Dei Delitti e Delle Pene,* Beccaria observed in 1764 that "finding nowhere a span of earth where real crimes were pardoned might be the most efficacious way of

[1] Robert Anderson, FBI: http://www.reuters.com/article/2014/05/14/us-cyber-summit-fbi-idUSBREA4D0UP20140514 (Accessed 20/12/2014).
[2] Schwarzenberger (1976), 46.
[3] Magnuson (2012), 851.
[4] Oppenheim (1955), 504.
[5] Magnuson (2012), 852.

preventing their occurrence."[6] Such a situation is yet to be realised, although some of the more active countries in the extradition field are certainly steadily on course to achieve this target through means of bilateral treaties.[7] The globe shrinks even further when multilateral extradition conventions, or other surrendering arrangements,[8] and the extradition provisions of suppression conventions, are taken into account.[9] But this shrinking in the number of extradition havens is occurring while other spatial considerations are expanding, namely the number of countries that can be simultaneously affected by criminal conduct, and their respective territorial rules of jurisdiction.[10] Beccaria's advocacy of extradition was in the context of refuting claims that States could punish crimes regardless of the place of commission, "as if a man could live in one country and be subject to the laws of another, or be accountable for his actions to two sovereigns, or two codes of laws often contradictory."[11] For Beccaria, it was seen as elementary that the only country that could punish a crime is that where the crime was committed,[12] and extradition was thus the only means to do so if a fugitive had escaped to another country. Definitions of extradition in the early 20th century equally presupposed such an uncomplicated world of crime and territoriality.[13] However, the world as Beccaria knew it is long gone. A man now can live in one country, and be subject not only to the laws of two sovereigns, but to many others as well.

In this chapter I first provide a brief introduction to the general structure of extradition law, and the inherent tensions for States existing therein, beginning with an analysis of the attempted extradition of Gary McKinnon. I then trace

---

[6] Farrar (1880), 194.
[7] Both the US and the UK have bilateral extradition treaties with over one hundred countries. For the US, see Appendix 1 of Garcia and Doyle (2010) for a recent list of such countries. For the UK, see https://www.gov.uk/extradition-processes-and-review (Accessed 20/12/2014).
[8] E.g. the European Convention on Extradition 1957 (CETS No. 24, 13 December 1957) (**the European Convention on Extradition**), and European Arrest Warrant Decision (2002/584/JHA, 13 June 2002) (**the European Arrest Warrant Decision**).
[9] See chapter three, section 3.4.3.
[10] See chapter five.
[11] Beccaria (1992), 84.
[12] Ibid, 85.
[13] Extradition was explained in one US case as "[t]he surrender by one nation to another of an individual accused or convicted of an offence outside of its own territory, and within the territorial jurisdiction of the other, which, being competent to try and punish him, demands the surrender." See *Terlinden v Ames* [1901] 184 US 270, 289.

the UK's historical treatment of jurisdictional concurrency in extradition cases, in order to explicate the forces which led to recent domestic structures. My fifth section discusses a number of recent cybercrime extradition cases, considering some of the political and normative difficulties which have ensued, and which threaten to become broader problems as States' investigative capacities increase. I will then consider some of the causes of the emerging difficulties, and the response of the United Kingdom to recent cybercrime extradition cases. I argue that the present paradigm, which entails breadth of territorial jurisdiction and trajectories in extradition law towards removal of barriers to cooperation, risks undermining the suppression project in the long term. McKinnon's case serves as the backdrop to explore this contention.

7.2 Gary McKinnon: A Representative Cybercrime Extradition Case?

The case of Gary McKinnon, a British national living in the UK, is renowned for being one of the longest running, protracted, and expensive extradition cases in British history, and was heavily relied upon by Brenner to make her case that extradition is "little, if any, use"[14] in cybercrime enforcement. McKinnon's case was said to be "representative"[15] of cybercrime extradition cases, and it will therefore be described at some length in this section.

McKinnon's alleged criminality dates from 2001, when he gained unauthorised access to 97 computers owned by the US Government, all of which was done from his home in the UK.[16] Pursuant to an MLA request, his computers were seized and provided irrefutable evidence of McKinnon's role in most of the above. He was interviewed twice during 2002, and admitted responsibility for the intrusion and the direct targeting of US Government computers.[17] In November 2002, he was indicted by a Grand Jury in the Eastern District of Virginia for seven counts under the Computer Fraud and Abuse Act,[18] with the

[14] Brenner (2014), 44.
[15] Ibid, 45.
[16] See the facts as recounted in *Gary McKinnon v Government of the USA and Secretary of State for the Home Department* [2007] EWHC 762.
[17] Ibid, [8].
[18] 18 USC § 1030. See *US v Gary McKinnon* (Indictment, Eastern District of Virginia, November 2002).

US attorney responsible for indicting him describing it at the time as the "biggest military computer hack of all time."[19] However, despite the gravity of what was being alleged, almost four years passed before an extradition hearing was held in the UK. This was a result of, *inter alia,* complex and intensive analysis of the evidence by the US, direct negotiations between the US and McKinnon concerning the possibility of him voluntarily travelling to the US (which failed), and the passing of the Extradition Act 2003 (**EA 2003**) in the UK, which prompted the US to re-formulate its extradition request pursuant to the new statutory regime.[20] When the case eventually came before District Judge Evans in 2006, McKinnon raised a number of arguments against his extradition including various human rights points, and that the conduct must have occurred exclusively in the territory of the requesting State in order to constitute an extradition offence under the EA 2003. All of these arguments were rejected and his extradition ordered by Judge Evans and the Home Secretary shortly thereafter.

Before the year was out, however, McKinnon's lawyers were back in court, having brought appeals against both the decision of the District Judge and the Home Secretary. Numerous grounds of appeal were formulated, including that Article 8 of the ECHR (the right to privacy) would be infringed due to, *inter alia*, the likely duration of sentence which he faced in the US, and the proportionality of a foreign trial and sentence, given that he could have been prosecuted in the UK. The High Court rejected both limbs of the argument, referring to Canadian jurisprudence that an individual "must generally accept the laws and procedures of the countries they visit",[21] thus equating a 'cyber' visit with a physical visit.[22] On the proportionality point, the Court cited with approval the words of the District Judge:

> The CPS did consider whether to launch a prosecution in the UK and for good reason decided against it … It is not my task to determine which state has the

[19] http://www.guardian.co.uk/world/2012/oct/16/gary-mckinnon-timeline-extradition (Accessed 20/12/2014).
[20] For further detail of the early stages of his extradition case, see *McKinnon*, supra note 16, [21].
[21] *Ferras v USA* [2006] 2 SCR 77, [86].
[22] *McKinnon* [2007], *supra* note 16, [34].

> better right to prosecute, but for what it is worth my view is, unquestionably, if the defendant is to face prosecution, it should be in the US.[23]

All other grounds of appeal suffered a similar fate, as did his appeal to the House of Lords which concerned the plea bargaining undertaken,[24] and in the ordinary course of events, that would have been the end of the already lengthy saga: McKinnon had exhausted the EA 2003 appeal process, raised a range of arguments against his extradition, had lost at every stage, and looked to be *en route* to the US. But that was not the end of the matter. In August 2008, shortly after the decision of the House of Lords, he was diagnosed with Asperger's Syndrome. Appeals to the European Court of Human Rights[25] (**the ECtHRs**) and the then Home Secretary (Jacqui Smith) ensued on the grounds that his extradition would infringe Article 3 of the ECHR. Both again failed,[26] but McKinnon again persevered. He brought a judicial review of the Home Secretary's decision, and the decision of the DPP not to prosecute him in the UK.[27] On the latter, Stanley Burnton LJ again agreed, *obiter,* with the comments of District Judge Evans that the US was manifestly the right forum for prosecution,[28] and held that the DPP was under no obligation to prosecute him in the UK so as to prevent his ECHR rights from being infringed; it was for the Courts and the Secretary of State to entertain such claims.[29] The judicial review of the Home Secretary's decision also failed. Despite recognising that "[his] mental health will suffer … [and there] are risks of worse, including suicide",[30] Stanley Burnton LJ found that his case was not sufficiently severe to warrant the prevention of his extradition under Article 3 of the ECHR. The Home Secretary, then Alan Johnson, again reconsidered his medical evidence and his extradition was again ordered in November 2009. Another judicial review followed, which was adjourned before a hearing could occur because of a change of government, with Theresa May assuming the reigns as Home

[23] *Per* District Judge Evans, quoted ibid, [36].
[24] *McKinnon v USA* [2008] UKHL 59.
[25] He sought interim relief in the form of a stay under Rule 39.
[26] The Home Secretary's letter is quoted at some length in *McKinnon v Secretary of State for Home Affairs; McKinnon v DPP* [2009] EWHC 2021, [21].
[27] Ibid.
[28] Ibid, [45]-[46].
[29] Ibid, [55]. See, however, section 7.6 below regarding the review powers of the Home Secretary relating to human rights being removed.
[30] Ibid, [89].

Secretary. May spent two years making her decision and finally, on the 16th October 2012, she withdrew the extradition order concluding that his "extradition would give rise to such a high risk of him ending his life that a decision to extradite would be incompatible with Mr McKinnon's human rights."[31] She also simultaneously announced fundamental changes to UK extradition law, which will be discussed below.[32] In the end, McKinnon didn't even face trial in the UK, despite having admitted much of the conduct. This was due, apparently, to the difficulty of transferring evidence from the US and garnering the participation of US witnesses.[33] The DPP concluded that "the prospects of a conviction against Mr McKinnon which reflects the full extent of his alleged criminality are not high."[34]

This was an exceptional extradition case. By the time May withdrew the extradition order, McKinnon's various arguments had been considered by three Home Secretaries, a District Court Judge, the High Court (twice), the House of Lords and the European Court of Human Rights, and his case was even twice directly discussed by Prime Minister Cameron and President Obama. Nevertheless, Brenner regards it as "representative"[35] of cybercrime extradition cases, contending, *inter alia*, that it illustrates the fact that States are loathe to extradite their nationals, that a contributory factor for his non-extradition was that the perpetrator was never 'in' the US, and she ultimately uses the case to support her thesis that cybercriminals do not usually face justice.[36] Certainly, if such procedural complexity inhered in all cybercrime extradition cases, the end would be nigh for enforcement prospects.

I have begun this chapter with a description of the McKinnon case because I agree it is illustrative of many issues pertaining to cybercrime extraditions, but I wish to turn Brenner's analysis on its head, providing a different perspective as to why—and of what—it is representative. First, the case shows the ease of commission of cybercrimes in foreign countries, and that States will and can

[31] https://www.gov.uk/government/news/theresa-may-statement-on-gary-mckinnon-extradition (Accessed 20/12/2014).
[32] See section 7.6.
[33] http://blog.cps.gov.uk/2012/12/gary-mckinnon.html (Accessed 20/12/2014).
[34] Ibid.
[35] Brenner (2014), 45.
[36] Ibid, 49.

use extradition where this occurs, and *contra* Brenner, I argue it *is* of use in cybercrime enforcement actions.[37] While McKinnon was never prosecuted, recent cybercrime extradition cases suggest that this is the exception, not the rule, where treaties are in force. Extradition is used to prosecute perpetrators for crimes committed, but also to deter future offenders, and as investigative and enforcement powers expand these policies can be expected to be pursued more heavily. Second, leaving aside which country was the proper forum in the case, it demonstrates that in cases of jurisdictional concurrency, the lack of procedural harmonisation of criminal justice systems means there can be profound consequences for the defendant, depending on place of punishment. McKinnon faced a much higher penalty in the US[38] than he likely would have received in the UK, and if prosecuted in the former, would have been incarcerated far from family, friends, and familiarities. Third, the case is illustrative of US prosecutorial aggression, and the lengths their LEAs will go to in order to secure a suspect's extradition,[39] and it demonstrates that determinations made by TGNs (e.g. decisions whether to prosecute or not) can create significant, unexpected, difficulties for States, generating political potency even between countries that are self-regarded as 'strong allies.' Fourth, the McKinnon case is representative of the fact that there has been a movement in extradition law, which I will trace in the literature and with the UK as a case

[37] This will be demonstrated in section 7.5 below, and this must also be seen in the context of a significant rise in the use of extradition in criminal enforcement. The US received and sent fewer than fifty extradition requests a year in the early 1970s, but this number increased ten-fold by the mid 1980s. See Garcia and Doyle (2010), page 1, footnote 3. Between the US and the UK alone, for the period 2004-2011, the US made 130 extradition requests, while the UK made 54. See Scott Baker, David Perry, and Anand Doobay, 'A Review of the United Kingdom's Extradition Arrangements' (Home Office, 2011), 472 (**the Baker Review**). Admittedly, the US is one of the most active countries in this field, and the numbers are not as high for other countries.

[38] The prospect of McKinnon facing seventy years in prison was referred to repeatedly in comments on his case: http://www.dailymail.co.uk/news/article-1158173/Pentagon-hacker-faces-70-years-US-jail--CPS-wont-try-Britain.html (Accessed 20/12/2014).

[39] I will not deal with other practices for gaining custody over individuals, such as extraordinary rendition, as it is obviously not addressed in suppression conventions. This is well known to be used by the US in terrorism cases (see e.g. the ECtHRs' decision in *Al Nashiri* (No. 28761/11, 24 July 2014), but less known is the fact that it is has also been practiced in cybercrime cases. See e.g. the on-going case against Roman Seleznev (*US v Zolotarev and others* Criminal Indictment 2:12-CR-604 (Nevada, December 10 2012)), who is suspected of involvement in the Carder.su forum. Seleznev is the son of a Russian politician who, while on holiday in Guam, was seized by US authorities, forcefully transferred to the Maldives, and then extradited to the US. See http://www.theguardian.com/world/2014/jul/08/russia-mps-son-seleznev-arrest-us-secret-service (Accessed 20/12/2014).

study, towards the expedition of the extradition process, which often precludes challenges on the grounds of nationality or forum; the latter argument was awkwardly shoehorned into human rights challenges in the McKinnon case and there was, therefore, little space for discussion or argument of the jurisdictional issues. This has resulted in a recent change of law in the UK, from which there are broader lessons for other countries, and for the suppression project. In order to quell the rising tide of transnational crime, States have utilised the malleability of the concept of territorial jurisdiction, and are—and are being urged to in suppression conventions—expediting and simplifying the extradition process, seeing it as a crucial cog in their collective response and responsibilities. When these processes are combined, however, the UK experience exposes the creation of an extradition train that can be difficult to stop. The compulsion to mutually surrender, even when the underlying jurisdictional nexus of the requesting State is tenuous, generates forces which may ultimately hamper cooperation, and the suppression project, in the long term.

7.3 Searching for Balance: Flexibility and Obligation in Extradition Law

The term 'extradition' has come to signify "the formal legal process by which persons accused or convicted of crime are surrendered from one State to another for trial or punishment."[40] Although it is a word which was apparently only first used in a treaty in 1781,[41] which is surprising given that it is a practice of such antiquity, such treaties have since then become ubiquitous. The UK, for example, has extradition relations with over one hundred countries across the world, due either to bilateral treaties or multilateral conventions and other agreements, such as the London Scheme.[42] Common international practice is to require not only a treaty, but also domestic implementing

[40] Baker Review (2011), *supra* note 37, 20.
[41] Wijngaert (1980), 5.
[42] Extradition between Commonwealth countries, for example, is based on the Scheme for the Rendition of Fugitive Offenders within the Commonwealth, agreed by the Commonwealth Law Ministers in April-May 1966. The Fugitive Offenders Act 1967, which repealed its 1881 predecessor, was based on this scheme. Extradition with many countries is still governed by this scheme. See the Baker Review (2011), *supra* note 37, 268-270.

legislation enumerating the specificities and practicalities of extradition arrangements.[43]

The motivation for choosing one arrangement over another can be difficult to distil. The majority are based on bilateral treaties which Blum argues is the best way of regulating this activity between States.[44] This is because "differences among countries are materially relevant to the regime";[45] States would not, for example, want to extradite "their citizens to all countries without distinction."[46] Looking at UK extradition law, where some countries have to meet a higher evidential threshold for extradition depending on its designation by the Secretary of State,[47] this certainly rings true. Moreover, Blum claims, extradition arrangements "impose almost no externalities on third parties."[48] In other words, States not involved in the extradition are not affected by the activity. While the transaction costs of negotiating numerous bilateral treaties are high, they outweigh the cost of attempting to find a universally agreeable solution. Multilateralism in the context of extradition, she argues, is "bound to fail."[49]

Magnuson, however, argues that this explanation fails to take into account the role of domestic politics in State decision-making. Externalities arise, for example, when domestic groups in a third country take interest in an extradition due to their citizen being involved.[50] Moreover, while it is true that multilateral conventions dealing exclusively with extradition are fairly thin on the ground, there are notable exceptions.[51] Equally noteworthy are provisions in suppression conventions which deem the suppression offences extraditable offences in existing instruments, and, importantly, also allow Parties to treat

[43] McNair (1956), vol II, 41.
[44] Blum (2008), 361.
[45] Ibid, 360.
[46] Ibid.
[47] Under the EA 2003, a category two country does not need to establish "*prima facie*" evidence, if it has been so designated under s.84(7).
[48] Blum (2008), 361.
[49] Ibid, 360.
[50] Magnuson (2012), 874.
[51] European Convention on Extradition, Arab League Extradition Agreement (BFSP 159, 14/9/1952), Benelux Extradition Convention (616 UNTS 8893, 27/06/1962), Inter-American Convention on Extradition (1752 UNTS 191, 25/02/1981), European Arrest Warrant Decision. For discussion of the constitutional and political challenges which arose from this last arrangement see Deen-Rasmany (2006) and Sliedregt (2007).

the convention itself as an extradition treaty, if one State makes extradition conditional on such an instrument.[52] Countries like the US have agreed a huge number of bilateral extradition treaties,[53] and have traditionally been averse to multilateral extradition treaties,[54] but they have been prominent proponents of suppression conventions, which contain extradition provisions.

Therefore, any attempt to provide a coherent and comprehensive explanation of the motivations for particular forms of extradition relationships will struggle due to, *inter alia,* the diversity of arrangements. Moreover, theories which more broadly discuss the motivations for States entering treaties lose some of their explanatory appeal when transposed to the extradition realm. Guzman's rational choice model,[55] for example, would look to the costs and benefits of agreeing a treaty, as opposed to a soft law arrangement such as the London Scheme.[56] For Guzman, the costs of a treaty might be the increased reputational harm in the case of a refusal to extradite as agreed, as against the increased likelihood of reciprocal return of criminals. But even at an abstract level, there are difficulties with the simplicity of Guzman's account. As noted in chapter three, Brewster, for example, complicates the idea that reputational harm can serve as a constraining force on State behaviour,[57] while Kydd points to the importance of domestic politics in influencing international conduct, which was largely neglected by Guzman.[58] As we shall see, both have proved, in light of recent UK extradition decisions, to be incisive critiques. Theresa May may well have considered the long term reputational harm for the UK generated by her refusal to extradite Gary McKinnon, [59] particularly because her interpretation of Article 3 of the ECHR contradicted the decisions of two previous Home Secretaries, the High Court, the ECtHRs, and her own decision

[52] See discussion in chapter three, section 3.4.3, and Article 24(2)&(3) Cybercrime Convention. See also how Australia has transposed Article 24(3) in reg. 5 Extradition (Cybercrime) Regulation 2013 (No. 3 of 2013).
[53] Appendix 1 of Garcia and Doyle (2010).
[54] Nadelmann (1993), 410.
[55] See chapter three, section 3.3.
[56] Guzman (2008). On the 'hard' versus 'soft' law dichotomy within the context of EU law, see Trubek and Trubek (2005).
[57] Brewster (2009).
[58] Kydd (2009). See, however, Guzman (2009).
[59] The US government spoke openly about its anger and surprise regarding May's decision. See the comments of Lanny Bruer, US Assistance Attorney General. Available at: http://www.telegraph.co.uk/news/uknews/law-and-order/9629768/Gary-McKinnon-US-official-very-disappointed-over-decision-to-block.html (Accessed 20/12/2014).

to extradite Talha Ahsan who suffered from the same condition,[60] a little over a week earlier. Domestic political forces were undoubtedly responsible for her decision: McKinnon's friends and family mounted a powerful media campaign that ultimately made his extradition politically impossible. National newspapers were replete with articles speaking of the need to protect British citizens from extradition,[61] and politicians such as David Cameron[62] (before coming to power), and Nick Clegg[63] spoke openly about their opposition to US trials.

More can be learnt, however, from an analysis of the content of extradition structures; even a glance at such arrangements reveals a consistent struggle by States to build appropriate flexibility and safeguards into their arrangements, whilst simultaneously maintaining the credibility of their commitments. Flexibility ensures that States can re-evaluate their obligations if, for example, the political situation changes in the territories of their extradition partners, or the latter introduces criminal laws that are repulsive domestically. It ensures that in the face of new, unforeseen problems, they will be able to re-evaluate their situation, and will not be held responsible for punishments that could generate outrage at home.

For this reason UK extradition law has, for most of its history, provided the Home Secretary with a general discretion to refuse extradition in any given case.[64] However, such a general discretion challenges the idea behind an extradition treaty generating obligations, and does little to reassure other States that their treaty will not be broken in politically sensitive cases. It weighs the value of cooperation and the need to assure other countries of their commitments against the need to retain flexibility, and comes down in favour

[60] See below, section 7.5.Cybercrime Extraditions
[61] See e.g. http://www.guardian.co.uk/commentisfree/2012/jun/04/gary-mckinnon-extradition (Accessed 20/12/2014)
and http://www.huffingtonpost.co.uk/2012/10/05/babar-ahmad-justice-syed-talha-ahsan-extradition_n_1943049.html (Accessed 20/12/2014).
[62] http://news.bbc.co.uk/1/hi/uk/8178321.stm (Accessed 20/12/2014).
[63] http://www.dailymail.co.uk/debate/article-1198466/Nick-Clegg-This-vulnerable-man-hung-dry-government-desperate-appease-America.html (Accessed 20/12/2014).
[64] See e.g. s.11 Extradition Act 1870, s.6 Fugitive Offender's Act 1881 and s.12(1) Extradition Act 1989.

of the latter. But as the (perceived[65]) threat of transnational crime increased, this changed. As Magnuson notes, "extradition has become a legalized phenomenon in which discretion is highly cabined."[66] The decision-making process is increasingly becoming an almost entirely judicial affair, where extradition is mandatory provided certain minimum legal requirements are met. Flexibility became relegated as "[c]ountries appear to be willing to make irrevocable commitments to extradite suspected criminals to other countries."[67] And this ceding of discretion not only enhances the credibility of its commitments, but it also insulates the executive from public criticism in contentious cases. Nowhere is this clearer than in the EA 2003, where the Secretary of State saw a drastic reduction in her role in the extradition process, including the removal of her general discretion, and there are now only very limited considerations upon which she can refuse extradition.[68] Moreover, after the McKinnon affair, her role has been reduced even further. Much of the latter stages of McKinnon's case arose because he raised human rights appeals relating to his medical condition before various Home Secretaries, which had to be considered given their status as public authorities under the Human Rights Act 1998. Once bitten, twice shy. In the future, appeals against extradition orders on human rights grounds, after the permitted period for appeal, can only be brought before the High Court, and only then if the grounds are exceptional or raise the prospect of "real injustice" if not considered.[69]

Of course, this general executive discretion was but one form of flexibility built into extradition relations, and many other tools were developed over the years which continue to be found in treaties and domestic law. Human rights law grants considerable judicial discretion to refuse extradition, but has been

[65] See e.g. Andreas (2013), who argues that the depiction of porous borders and out-of-control crime threats suffers from historical amnesia, implying that such borders were actually once under control.
[66] Magnuson (2012), 877.
[67] Ibid.
[68] In the context of category two territories (non-EU), the bars upon which she can prohibit extradition relate only to issues such as whether the death penalty may be imposed, or speciality, which requires that the requesting country only prosecutes for the crimes specified in the extradition request. See ss.94-96A EA 2003. It was also recommended in the Baker Review (2011), *supra* note 37, para.1.32 that that her powers under the EA 2003 should not be increased.
[69] See s.50 and Schedule 2, Part 2, Crime and Courts Act 2013.

tightly interpreted in this context.[70] In fact, looking across traditional extradition considerations for countries, one can deduce a definite move towards the facilitation of cooperation. As Nadelmann has argued, "where once extradition treaties were negotiated with a keen sense of their intended limits, today they are increasingly designed to be highly open-ended."[71] The rule against double criminality, for example, states that "…no person is to be extradited whose deed is not a crime according to the criminal law of the State which is asked to extradite, as well as of the State which demands extradition."[72] This ensures that States will not be forced to assist "in the enforcement of criminal laws unknown in its own domestic legal order."[73] However, rules that developed as a result of such concerns, have been altered over the years, due to insufficient flexibility. In the 19th century the extradition treaties agreed by the UK enumerated the specific offences that were extraditable under the agreement.[74] When extraditions began to be impeded due to technical issues of legal classification, a 'no-list' system was developed in the 20th century.[75] This allows for extradition of all offences, regardless of how it is described in the respective countries, provided it meets a certain minimum level of gravity, measured by periods of imprisonment.[76]

The citizenship/nationality exception has similarly been chipped away at over the years. This rule simply prohibits the extradition of nationals, and was even described as a "right" in Article 6 of the European Convention on Extradition 1957. Traditional justifications have been that:

> (1) the fugitive ought not be withdrawn from his natural judges; (2) the state owes its subjects the protection of its laws; (3) it is impossible to have complete confidence in the justice meted out by a foreign state, especially with regard to a foreigner; and (4) it is disadvantageous to be tried in a foreign language, separated from friends, resources and character witnesses.[77]

---

[70] See e.g. *Ahmad and others v UK* [2012] ECHR 609 in the context of Article 3 ECHR.
[71] Nadelmann (1993), 458.
[72] Oppenheim (1955), 701.
[73] Baker Review (2011), *supra* note 37, 36.
[74] See e.g. Article 10 of the Webster-Ashburton Treaty (9 August 1842).
[75] Stanbrook and Stanbrook (2000), 1.21. For discussion of a similar trend in the US context, see Nadelmann (1993), 411.
[76] See e.g. the definition of extradition offences in ss.137-138 EA 2003.
[77] Williams (1991), 260-1, quoting the findings of Sir Alexander Cockburn CJ's Royal Commission Report of 1877.

These justifications have never been regarded as compelling in the UK,[78] being seen as a form of legal xenophobia and "resting upon sentimental considerations and an exaggerated notion of the protection which is due by a state to its subjects."[79] While such bars can certainly still be found in some countries, there have been significant efforts to curb reliance on them, which has been yielding results, most notably in the fact that it is not a legitimate ground for refusal of a European Arrest Warrant.[80] However, one of the areas where States have consistently struggled to achieve the appropriate balance between maintaining discretion and ensuring credibility in their obligations is in dealing with extradition requests where the requesting State is relying on extraterritorial jurisdiction, or tenuous territorial connections. This is particularly the case when the requested State could also prosecute the offence. Although this is an issue with roots dating from the very inception of the extradition relationship between the UK and US,[81] it has been significantly exacerbated with the advent of cybercrime, and compounded, for some countries, by the gradual erosion of rules like the nationality exception.

During the 19th and early 20th centuries, States gradually became alert to the difficulties which can emerge from such extradition requests, and dealt with it in their domestic statutes and extradition treaties in two main ways. First, either in domestic law or in bilateral treaties, States often required that extradition could only occur if the requesting State had territorial jurisdiction.[82] This was an indirect way of dealing with the problem of concurrent jurisdiction between requesting and requested parties in extradition cases,[83] and prevented States

[78] One exception was an extradition treaty between Switzerland and Great Britain, which resulted in the discharge of an alleged fugitive. See *R v Wilson* (1877) 2 QBD 42. Cockburn CJ, however, characterised it as a "blot upon the law", and the 1877 Report recommended that it should not form part of domestic extradition law.
[79] Moore (1891), section 127.
[80] For discussion see Deen-Racsmány and Blekxtoon (2005). Non-EU countries have also parted ways with the exception, often under pressure from the US. See Johnson (2005), 211, discussing the case of Columbia.
[81] For an excellent account of the extradition of Thomas Nash in 1799, from the US, pursuant to the Jay Treaty of 1794, see Wedgwood (1990).
[82] See e.g. the list of bilateral treaties referred to by Bedi (1966), 63, footnote 9. Bedi (1966), 175, footnote 43 also lists some domestic provisions containing similar stipulations. Some multilateral conventions contain similar provisions: see e.g. Article 8(1) of the Asian-African Convention on Extradition 1961 (VI, 338).
[83] Given the ease of claiming territorial jurisdiction in cybercrime cases, it would also be an ill-equipped tool to deal with primary concern of States in such cases, which is another State prosecuting a crime which the requested State also has an interest in prosecuting.

from exercising extraterritorial jurisdiction. As a result, such provisions have in many instances been replaced in conventions,[84] bilateral treaties,[85] and domestic law,[86] with provisions which intertwine dual criminality considerations with these jurisdictional concerns. In other words, they generally allow States to extradite in relation to extraterritorial offences, unless the requested State does not recognise extraterritorial jurisdiction for such offences under its domestic law.[87] A second, more direct, way of dealing with this was to provide in extradition statutes or treaties that extradition would not be granted for offences committed within the requested State's territory.[88] Such provisions were seen to be "[i]n conformity with … [the] principle of territorial competence"[89] and in one draft of a proposed extradition convention it was even said to be a 'rule' that extradition would not be granted when the offence was committed within the requested State.[90] However, in the Harvard Research Draft Convention on Extradition it was not stated so categorically, and was suggested as an optional ground for refusing extradition, when the act was committed in whole or in part in the requested State's territory.[91] Such a provision has subsequently made its way into multilateral conventions,[92] but by the beginning of the 21st century, the position in the UK was that jurisdictional concurrency was no reason to bar extradition. The reasons for this will be explored in the next section, but what should be clear from the above is that while extradition is an area where States have battled to build appropriate flexibility and safeguards into their arrangements,[93] the "modern era"[94] of

[84] Article 7(2) European Convention on Extradition and Article 4(7)(b) European Arrest Warrant Decision.
[85] See Article 2(4) US-UK Extradition Treaty (31 March 2003).
[86] See e.g. s. 3(1)(c) Fugitive Offenders Act 1967 (now repealed). See now s.64(4) of the EA 2003.
[87] See also Article 3(b) of the Harvard Draft Convention on Extradition: Harvard Research in International Law, 'Extradition', *American Journal of International Law*, 29 Supplement, (1935).
[88] For a list of such provisions in domestic law, and bilateral treaties, see Bedi (1966), 63, footnotes 7-8.
[89] Bedi (1966), 175.
[90] See the Model Draft prepared by the International Penal and Prison Commission, at Article 4: Harvard Research on Extradition (1935), *supra* note 87, Appendix IV, at 310.
[91] See Article 3(a).
[92] See e.g. Article 7(1) European Convention on Extradition, Article 2(3) of the Inter-American Convention on Extradition and Article 4(7)(a) European Arrest Warrant Decision.
[93] Magnuson (2012), 879.
[94] Defined by Nadelmann (1993), 410, as the period since 1970 in the context of the US.

extradition practice can often be characterised as erring on the side of cooperation and facilitation. As Nadelmann notes in the US context:

> negotiators have sought to maximize the number of offences for which a treaty partner will extradite; to narrow as much as possible the 'political offense' exception … ; *to accommodate the extraterritorial reach of U.S. and foreign criminal laws and jurisdictional notions*; to persuade foreign governments to extradite their nationals…[95]

7.4 Dealing with Jurisdictional Concurrency in UK Extradition Law

While the UK now has over one hundred extradition agreements with different countries,[96] it is to be remembered that it is still a relatively recent phenomenon in the English legal system; England only concluded five extradition agreements between 1174 and 1794,[97] and only three between 1842 and 1868.[98] Modern extradition law in the UK can therefore be traced to the mid-19th century when treaties were agreed with the US and France,[99] and which were followed by a range of domestic statutes dealing with extradition between the UK and Commonwealth or other third countries: the Extradition Acts 1870-1935, the Fugitive Offenders Act 1967 (and its predecessor from 1881), certain provisions in the Criminal Justice Act 1988, the Extradition Act 1989 (**the EA 1989**), and most recently, the EA 2003. An analysis of these statutes reveals a variety of constructs and processes for dealing with concurrent jurisdiction in extradition cases, with the UK having gone from a restrictive position, where extradition was refused in cases of concurrency, to a much more permissive regime. This occurred as part of a recent movement to drastically expedite and simplify the extradition process, which is expected in transnational crime conventions like the Cybercrime Convention, in the fight against transborder crime.

In the mid 1800s the prevailing view in the UK was that only individuals sought for crimes committed *exclusively* within the territorial jurisdiction of the

---

[95] Nadelmann (1993), 410. Emphasis added.
[96] https://www.gov.uk/extradition-processes-and-review (Accessed 20/12/2014).
[97] Clarke (1903), 18-22.
[98] With France, the US and Denmark. See Baker Review (2011), *supra* note 37, 28.
[99] See e.g. the Webster-Ashburton Treaty of 1842, and the Treaty between Great Britain and France of 1843.

requesting State could be subject to extradition. The 1842 Treaty with the US, which was implemented by the Extradition Act 1843, allowed for extradition for crimes "committed within the jurisdiction" of either State, and this was very narrowly interpreted in *Tivnan*.[100] Three men were sought for an act of piracy (one of the crimes enumerated in the 1842 Treaty) on board an American ship, but the majority held that they could not be extradited because the crime had not been committed within the "peculiar",[101] or "exclusive"[102] jurisdiction of the US. Piracy *jure gentium* was prosecutable by all States and the fact that the UK could do so in the case at hand was a significant factor in the decision.[103] Crompton J found it "very difficult to my mind to suppose that two of the great maritime nations of the world meant to give up their power of trying pirates wherever they were caught."[104] Shee J also thought it "injurious" to suppose that a State would "bind … itself to surrender to the justice of another state persons charged with the commission of crimes which it would be the duty of both to punish, and over which both would have jurisdiction."[105]

Four years later, these words must have been in the minds of the drafters of the Select Committee Report on Extradition of 1868, which only envisaged surrendering "to any foreign Government within whose jurisdiction such crime is alleged to have been committed."[106] And the proposal duly found its place in the Extradition Act 1870; only a "fugitive criminal" could be extradited, a term which was defined as "…any person accused or convicted of an extradition crime committed within the jurisdiction of any foreign state."[107] Confusion began because the words 'territory' and 'jurisdiction' were generally used

[100] *re Tivnan* (1864) 5 B & S 645.
[101] Ibid, 684, *per* Crompton J.
[102] Ibid, 691, *per* Shee J.
[103] Ibid, 689. The fact that piracy was included in the Treaty would seem to undermine the majority's opinions, but this was dealt with by distinguishing municipal piracy, from piracy *jure gentium*. Only crimes under the former jurisdictional ground were supposedly caught by the Extradition Treaty. The court shelved as irrelevant to the case before the court the fact that other instances of concurrent jurisdiction could arise, such as the US having territorial jurisdiction over a murder committed there, while the UK could prosecute because it was done by a British national. Ibid, 685, *per* Crompton J and ibid, 687-8, *per* Blackburn J.
[104] Ibid, 684-5, *per* Crompton J.
[105] Ibid, 691, *per* Shee J.
[106] Report of the Select Committee on Extradition of the House of Commons 1868, Command Paper 393.
[107] Extradition Act 1870, s.26.

interchangeably in treaties which the UK began agreeing after the 1870 Act,[108] and the narrow interpretation, which equated 'jurisdiction' with 'territorial jurisdiction', prevailed,[109] quite amazingly, until 2001.[110] However, in *Al Fawwaz* the Supreme Court unanimously decided that the definition of "fugitive criminal" should no longer be interpreted to allow extradition only in cases where the crime was committed in the territory of the requesting State. Their decision was heavily influenced by the current nature of many forms of criminality, which had not been envisaged at the passing of the 1870 Act. Lord Slynn said the restrictive interpretation "would make it impossible to extradite for some of the most serious crimes now committed globally or at any rate across frontiers"[111] and Lord Hutton also said this was the "principal reason"[112] for his decision. Concerns with other States asserting "exorbitant jurisdiction"[113] could be dealt with adequately through the general discretion of the Secretary of State.

In many respects, the U-turn by the Supreme Court was unsurprising; the Fugitive Offenders Act 1967 had, for Commonwealth countries and 'Her Majesty's Dominions', extended the jurisdictional grounds upon which a State could seek extradition, and pressure had been mounting since the 1980s for the UK to meet its "full responsibility for the maintenance of the international rule of law."[114] The EA 1989, therefore, also provided for extradition over extraterritorial offences, through the definition of 'extradition crimes.'

However, it soon became apparent that even these extradition procedures in the new legislation "were cumbersome, beset by technicality and blighted by

---

[108] Bedi (1966), 176.
[109] See e.g. *Kossekechatko v AG of Trinidad* [1932] AC 78. See also the *obiter* comment of Lord Mackay in *In re. Rees* [1986] AC 937, 955F where he said "[w]hen the 1870 Act was passed it dealt only with crimes committed within the territorial jurisdiction of a state with whom an extradition arrangement had been made."
[110] Although the EA 1989 had at this point consolidated all previous extradition acts, due to the complexities of the relevant provisions, extradition with the US prior to their 2003 Treaty and the EA 2003 coming into force, was still subject to provisions from the 1870 Act. See s.1(3) and Schedule 1 of the EA 1989.
[111] *R (Al-Fawwaz) v Governor of Brixton Prison* [2001] UKHL 69, [37].
[112] Ibid, [64].
[113] Ibid, [150], *per* Lord Slynn.
[114] Government White Paper, 'Criminal Justice: Plans for Legislation' (Cmnd. 9658, March 1986).

delay",[115] and despite a relatively brief existence in comparison to its predecessors, it was decided to radically alter domestic extradition law. In March 2001, a few months prior to the Supreme Court decision in *Al Fawwaz,* the Home Office published a review of the EA 1989, which recommended fundamental changes to domestic extradition law including, *inter alia,* a huge reduction in the role of the Secretary of State and a relaxation of the *prima facie* evidence requirement. Almost simultaneously, the EU was in the process of proposing the abolition of extradition between Member States, replacing it with a much quicker surrendering procedure.[116]

There was, therefore, a clear momentum towards expediting and simplifying the extradition process at the turn of the century, both within the UK and in the EU, and the EA 2003 was the direct result. This is an incredibly detailed and complicated act, with over two hundred sections and numerous schedules, and it has transformed the role of the executive and judiciary in the extradition process. But despite being born at the beginning of the Internet boom, the Act did little to address the issue of jurisdictional concurrency in extradition proceedings. In fact, safeguards against exorbitant claims to jurisdiction, which were seen as crucial by the Supreme Court only two years before (e.g. the general discretion of the Secretary of State to refuse extradition), were abandoned for the sake of reducing complexity, and duplicity in workload. And nothing was introduced in its place.

Like the Fugitive Offenders Act 1967 and the EA 1989, the only way the EA 2003 addresses concurrent jurisdiction and the jurisdictional grounds upon which extraditions could be sought, is in its definition of 'extradition crimes.' Any country seeking the surrendering[117] or extradition of an individual from the UK must demonstrate that the conduct for which extradition is sought constitutes an 'extradition offence', and the variants of this construct provide a number of safeguards (e.g. double criminality) which vary depending on whether the requesting State is exercising territorial or extraterritorial jurisdiction, and whether part of the crime was also committed in the UK.

[115] Baker Review (2011), *supra* note 37, para. 3.97.
[116] The European Arrest Warrant Decision.
[117] This applies to arrest warrants issued by EU States and is dealt with in Part 1 EA 2003.

However, when the detailed variants of extradition offences are dissected, it is clear that meeting this definition is usually merely a trivial task for requesting authorities. Extraditions sought either on territorial or extraterritorial grounds can proceed, even if the UK has territorial claims over the particular conduct.[118] The courts have confirmed as much in the context of concurrent territorial jurisdiction, under both Part 1 and Part 2 of the EA 2003.[119] It was even commented in one case that "[t]he fact that the conduct of each of these defendants, if looked at individually, might show that, say 95% of that conduct was within the United Kingdom and only 5% within the category 2 territory does not matter."[120]

It must have been foreseen that with this trajectory,[121] "conflicts involving mutual claims of jurisdiction appeared increasingly likely."[122] But the EA 2003, as originally enacted, allowed neither the courts nor the executive to decide, "where a criminal case is triable in either of two jurisdictions, which is the forum conveniens"[123] and the perception was that "extradition proceedings should not become the occasion for a debate about the most convenient forum for criminal proceedings."[124] Therefore, as the executive disempowered itself and transformed extradition into a judicial exercise where discretion is strictly curtailed and cabined, the possibility to raise questions as to forum was effectively rendered obsolete, with such arguments forced into legal channels (such as arguments related to Article 8 of the ECHR[125]) which were ill-

[118] In the case of Part 1 EA 2003, for example, this can be deduced from the fact that s.64(5) and s.65(5) both allow extradition on extraterritorial grounds, provided no part of the conduct occurred in the UK, but no such proviso is found in s.64(4) or s.65(5). This means extraditions can proceed under the latter provisions even if the UK is the only country with territorial jurisdiction.
[119] See e.g. Office of the King's Prosecutor, *Brussels v Armas* [2005] UKHL 67 and *R (Bermingham) v Director of the Serious Fraud Office* [2007] QB 727.
[120] *Per* District Judge Evans, decision of 25 June 2004, quoted in *Bermingham,* ibid, [43].
[121] This movement can also be discerned in bilateral treaties. Nadelmann (1993), 416 notes how "by the mid-1980s, new U.S. extradition treaties virtually eliminated the obstacles posed by differing jurisdictional notions, providing for extradition so long as the dual criminality requirement had been met."
[122] Ibid, 417.
[123] *Bermingham, supra* note 119, [57], *per* Laws LJ.
[124] *Norris v USA* [2010] UKSC 9, [67], *per* Lord Phillips.
[125] As in the case of the *McKinnon* extradition, and *Bermingham*, and most of the cases discussed in the next section.

equipped to deal with the substantive issues raised. But the extraditions had to go on. As Hale LJ has noted in an oft-quoted passage:[126]

> …there is a strong public interest in our respecting such treaty obligations. Such international co-operation is all the more important in modern times, when cross-border problems are becoming ever more common, and the need to provide international solutions for them is ever clearer.[127]

7.5 Cybercrime Extraditions

As mentioned in the introduction to this chapter, Brenner is of the view that extradition is of little use in the cybercrime context. Meanwhile the Supreme Court, in *Al Fawwaz*, feared that restricting extraditions only to cases where the requesting State was relying on territorial jurisdiction would significantly hamper international crime cooperation and the ability to extradite criminals for crimes committed 'globally' or 'across frontiers.'[128] My review of recent cybercrime extradition cases suggests that neither perspective is convincing. These cases also reveal that, unlike the McKinnon case, many recent extradition cases are much less clear-cut in terms of the appropriate forum for prosecution. They show that even if 'extradition crimes' were to be defined narrowly so as to allow extraditions only where the offence is committed in the territory of the requesting State, this is no longer a safeguard of any utility or a tool that can serve to resolve the normative issues which arise. This is demonstrated below in an analysis of some of the most high profile cybercrime extradition cases, all of which have been requested by the US.[129] However, I argue below that there are few grounds for European countries to criticise US practices in this regard, and many of the standard purported 'causes' of the difficulties which emerged between the US and, for example, the UK, do not stand up to scrutiny. Furthermore, although my problematisation of jurisdictional concurrency in cybercrime extraditions concerns only US practices—as the current cybercrime extradition kingpin—other countries could well be expected to begin adopting a more active role in this area in the future, particularly if their investigative and enforcement powers are expanded

---

[126] See e.g. *Bermingham*, *supra* note 119, [127].
[127] *R (Warren) v Secretary of State for the Home Department* [2003] EWHC 1177 (Admin), [40].
[128] *Al-Fawwaz, supra* note 111.
[129] This focus in my research is explained in section 1.4.

in the way proposed by the Transborder Group.[130] Therefore, while my problematisation of jurisdictional concurrency in this context is primarily concerned with the practices of one country, the theoretical possibility of it becoming a much more prevalent and widespread problem may require little to eventuate.

7.5.1. US to UK Extradition Requests

Beyond the McKinnon case, another recent cybercrime extradition case that received considerable attention in the UK involved Richard O'Dwyer, a student from Sheffield (**the O'Dwyer extradition**). He was sought by the US in relation to his role with various linking sites, which he operated from the UK. A complaint was filed in New York charging him with conspiracy to commit copyright infringement and criminal infringement of copyright. The complaint[131] and affidavit filed in support of his extradition[132] do not hide the fact that the US was but one of many countries which could have prosecuted in the case. The websites were "offer[ed] to the public throughout the world, including the United States…"[133] and were "viewed thousands or tens of thousands of times by individuals throughout the world, including the United States…"[134] Although the complaint could point to two alleged co-conspirators who were involved in the administration of the site being based in the US, it seems the primary jurisdictional grounds upon which the complaint was based relates to the accessibility of the site by investigating officers in New York.[135] But this was enough for his extradition to be ordered in the UK, as the District Judge made clear:

> There are said to be direct consequences of criminal activity by Richard O'Dwyer in the U.S.A. albeit by him never leaving the north of England. Such a state of affairs does not demand a trial here if the competent authorities decline to act and does, in my judgment, permit one in the U.S.A.[136]

---

[130] See chapter four.
[131] *US v O'Dwyer* (Complaint by Special Agent Di Laura, 10 Mag 2471, 5 November 2010).
[132] *US v O'Dwyer* (Affidavit of John Reh in Support of Request for Extradition, Criminal Case No. 10 Mag 2471, 23 February 2011)
[133] Ibid, [4].
[134] Ibid, [6].
[135] *O'Dwyer* complaint, *supra* note 131, [11] & [17].
[136] *USA v O'Dwyer* (Ruling of Purdy DJ, 13th January 2012), 9. O'Dwyer was not prosecuted in the end, but only because he travelled to the US with his lawyer and entered into a deferred

Although not charged with offences directly covered in the Cybercrime Convention, another case of note is that of Babar Ahmad and Talha Ahsan (**the Ahmad and Ahsan extraditions**). Both men were sought in separate indictments[137] for various terrorist offences in relation to their role with Azzam Publications and its family of websites. Allegedly, these sites were used to recruit individuals for the mujahedeen and to raise funds for the Afghani and Chechen divisions of the organisation. The indictments recognised that Azzam was "an entity based in the United Kingdom",[138] and that the websites operated "throughout the world",[139] with the defendants operating and maintaining the websites "in Connecticut, Nevada, the United Kingdom, Ireland, Malaysia *and elsewhere*…"[140] Presumably, these other countries were specified because aspects of the administration of the sites involved companies based there, but this merely demonstrates the diversity of countries implicated in the case, if jurisdiction is grounded on such tenuous connections. Nevertheless, the indictments alleged that the offences occurred "in the District of Connecticut *and elsewhere*…"[141] When their cases eventually went to the ECtHRs, the initial admissibility decision explained how this claim was substantiated: "the material support is alleged to have been provided through a series of websites whose servers were based in Connecticut."[142] In the judgment on the merits this sentence was repeated verbatim, except to downgrade it to say that only one of the servers was based there.[143]

There were undoubtedly other connections with the US in this case, such as the fact that Ahmad was alleged to have had US naval plans in his possession.[144] But unlike in the O'Dwyer extradition, where it wasn't even known in which country *TV Shack* was hosted,[145] the jurisdictional nub of this case was based

---

prosecution agreement with the US. See http://www.bbc.co.uk/news/uk-england-south-yorkshire-20525891 (Accessed 20/12/2014).

[137] *USA v Ahmad (*District of Connecticut, indictment, 6 October 2004) and *USA v Ahsan (*District of Connecticut, indictment, 28 June 2006).

[138] *Ahmad* indictment, ibid, [11].

[139] Ibid, [10].

[140] Ibid, [12], identical wording is used in the Ahsan indictment, *supra* note 137, [13]. Emphasis added.

[141] *Ahmad* indictment, [17], *Ahsan* indictment, [19], *supra* note 137, emphasis added.

[142] *Ahmad and others v UK* [2010] ECHR 1067, [5].

[143] *Ahmad and others v UK* [2012] ECHR 609, [10].

[144] *Babar Ahmad and others* [2012] EWHC 2736, [147]-[148].

[145] *O'Dwyer* affidavit, *supra* note 132, [12].

on the location of *one* of the servers, as was noted by the ECtHRs. Therefore, while the US could point to tenuous territorial connections, and extraterritorial jurisdiction based on the protective principle, it was but one of many countries that could have claimed an interest in the case. The extradition structure, however, provided no medium for these diverse interests to be considered, forcing the District Judge in the Ahmad extradition to admit:

> This is a difficult and troubling case. [Babar Ahmad] is a British subject who is alleged to have committed offences which, if the evidence were available, could have been prosecuted in this country. Nevertheless the Government of the United States are entitled to seek his extradition under the terms of the Treaty and I am satisfied that none of the statutory bars apply.[146]

A final illustrative case from the UK is that of Usman Ahzaz, a national of Pakistan, studying in the UK, and alleged to have controlled a botnet of over 100,000 compromised computers (**the Ahzaz extradition**). He was indicted in the District of Columbia with one count of damaging a computer or information "within the District of Columbia *and elsewhere*."[147] One of the issues discussed in his extradition hearing was the number of computers actually compromised in the US: "[a]fter some debate … it was established that, of those 100,000 computers, approximately 800 were physically located in the United States."[148] The jurisdictional nexus with the US in this case was, therefore, fairly thin. The alleged criminality was initiated in Pakistan and the number of computers compromised in the US was not even 1% of the entire number affected by the botnet.[149] But Ahzaz was also successfully extradited.[150]

7.5.2. US Extradition Requests Beyond the UK

The UK is far from the only country becoming accustomed to receiving extradition requests based on the territorial interpretations of jurisdiction described in the previous section. The Australian courts dealt with a case similar to the O'Dwyer extradition, involving Hew Raymond Griffiths, who was successfully extradited, and prosecuted in the US, in relation to his role in

---

[146] *Quoted in Babar Ahmad and others* [2012] EWHC 2736, [24].
[147] *Usman Ahzaz v The United States of America* [2013] EWHC 216, [8]. Emphasis added.
[148] Ibid, [7].
[149] The figure is possibly even smaller given that the FBI admitted that the code was ultimately installed on *more* than 100, 000 computers.
[150] http://www.thenews.com.pk/Todays-News-2-168098-Pak-computer-expert-extradited-to-US-on-hacking-charges (Accessed 20/12/2014).

an international 'warez' piracy group called "Drink or Die." He was indicted on two counts of conspiracy to infringe copyright, and copyright infringement as either a principal or accessory. The Federal Court of Australia, both on initial review,[151] and on appeal,[152] held that the extradition Magistrate's decision was wrong to have characterised Griffith's acts as having been physically committed in Australia, because conspiracy is a continuing offence. Even if the conspiracy was formed outside the US, there were said to be overt acts in the US when the relevant material was stored on a server there.[153] As a result, the offences could "properly be said to have occurred in the United States and this includes Mr Griffith's own conduct notwithstanding his actual presence in New South Wales."[154] The case has not, however, gone without its critics, even amongst the Australian judiciary. Soon after, New South Wales's Chief Judge in Equity noted:

> [i]nternational copyright violations are a great problem. However, there is also the consideration that a country must protect its nationals from being removed from their homeland to a foreign country merely because the commercial interests of that foreign country are claimed to have been affected by the person's behaviour in Australia and the foreign country can exercise influence over Australia.[155]

Location of Internet infrastructure, as in the Ahmad and Ahsan extraditions, has also featured heavily in a number of other cybercrime extraditions. In one of the most dramatised of cases, Kim Dotcom, as well as his companies (e.g. Megaupload Ltd) and associates, have been indicted in the Eastern District of Virginia for various copyright and racketeering offences, in relation to Megaupload, a very successful cloud storage site (**the Dotcom extradition**). The seizure of jurisdiction in this case again centred on the fact that one of the service providers from which Megaupload leased server space was based in the Eastern District of Virginia, and some of its data centres were also based there.[156] The jurisdictional grounds relied upon in this case have been robustly

---

[151] *USA v Griffiths* [2004] FCA 879, [121].
[152] *USA v Griffiths* [2005] FCAFC 34, [95]-[98].
[153] Ibid, [96].
[154] Ibid, [97].
[155] Young (2007), 225.
[156] *USA v Kim Dotcom and others* (Indictment, Eastern District of Virginia, Criminal No. 1:12CR3, filed 5 January 2012) [38], [53], & [65].

criticised in a White Paper,[157] prepared by two lawyers, one of whom is now acting for Dotcom. The Paper points to the fact that the organisation was located outside the US, that all defendants were foreign citizens resident abroad, that only about 10% of the users of the site were resident in the US, and that a substantial proportion of the data centres hosting the content on the site were located in The Netherlands, Canada, France, and other countries.[158] It concludes that:

> [t]he Megaupload prosecution demonstrates astounding hubris by the U.S. government, which has now moved to "colonize" the global Internet under its legal jurisdiction, without the slightest bit of respect for the sovereignty of other countries or their views about the boundaries of criminal liability for copyright infringement.[159]

This colonisation can also be seen in other cybercrime extradition cases—such as *Regpay*,[160] *Kolarov*[161] and *Bendelladj*[162]—where location of Internet infrastructure has again been central. In *Bendelladj*, for example, an Algerian national was extradited from Thailand for his role in developing and marketing a computer virus (SpyEye).[163] Once a computer is infected with this virus, it becomes a 'bot' which could be controlled through a command and control

---

[157] Amsterdam and Rothken (2013).
[158] Ibid, 34.
[159] Ibid, 36.
[160] This involved the redlagoon.com child pornography site, where citizens of Belarus were lured to France and Spain by US agents—since Belarus did not have an extradition agreement with the US—and then extradited. Although it was acknowledged that the individuals from Regpay maintained and operated the sites from Belarus, the indictment focused heavily on the fact that the redlagoon and other associated websites, as well as payment transaction records for the consumers, were hosted in the United States. For discussion see Sansom (2009), 223. See also: http://www.justice.gov/archive/opa/pr/2004/January/04_ag_021.htm (Accessed 20/12/2014).
[161] For background see:
http://www.justice.gov/usao/nj/Press/files/Kolarov,%20Aleksi%20Extradition%20PR.html (Accessed 20/12/2014).
Aleksi Kolarov was indicted in 2004 and eventually extradited to the US from Paraguay in June 2013 for his role in the Shadowcrew forum, an online marketplace which facilitated hacking, the acquisition of personal identifying and financial information, and various frauds. The site (www.shadowcrew.com) was hosted in New Jersey, where Kolarov and many others were indicted and prosecuted. In a separate case, Sergei Tšurikov was extradited from Estonia to the US, for hacking RBS WorldPay, headquartered in Georgia, where the servers are also based: *USA v Sergei Tšurikov* (Georgia indictment, 1:09-CR-491, November 10 2009).
[162] *US v Bendelladj* (Georgia indictment, No. 1:11-cr-557, 20 December 2011).
[163] SpyEye is a "malware toolkit specifically designed to automate the theft of confidential personal and financial information, such as online banking credentials." Ibid, [5]. For more information about the extradition see http://www.justice.gov/usao/gan/press/2013/05-03-13.html (Accessed 20/12/2014).

server, one of which was based in Atlanta, Georgia.[164] It was the location of this *one* server upon which the jurisdictional case was primarily built.[165] It was not clear, however, how many other command and control servers were being used in this botnet, or their location, but current estimates place the number at 165, the majority of which are not based in the US.[166] The indictment neither specifies the total number, and location, of other computers compromised by the malware, but it is likely to be millions spread across the world.[167]

This highlights the ease of mass victimisation in the online environment, as in the Ahzaz extradition, and looking across the numerous cybercrime extradition cases that are emerging in malware and fraud cases[168] the most common words in the US indictments refer to there being harm "in the United States *and elsewhere*";[169] but any amount of the former is enough for an extradition to proceed. Often indictments will only highlight a handful of victims in the US,[170] and although there may be many more victims in the US than are

---

[164] Ibid, [17].

[165] The indictment referred, for example, to communications between it and eleven other compromised computers (bots) based in various US States. Ibid, [21]. Various counts of computer access offences also concerned communications between the C&C server, and ten computers based in the US. Ibid, [29].

[166] https://spyeyetracker.abuse.ch/ (Accessed 20/12/2014). The indictment specified the total number, and location, of other computers compromised by the malware, but it is likely to be millions spread across the world: http://www.thetechherald.com/articles/Microsoft-smashes-Zeus-and-SpyEye-botnets-with-giant-RICO-bat (Accessed 20/12/2014).

[167] http://www.thetechherald.com/articles/Microsoft-smashes-Zeus-and-SpyEye-botnets-with-giant-RICO-bat (Accessed 20/12/2014).

[168] See e.g. Operation Open Market involving the carder.su website, where 55 individuals have been charged in four separate indictments, with many defendants based outside of the US: http://www.justice.gov/opa/pr/member-organized-cybercrime-ring-responsible-50-million-online-identity-theft-sentenced-115 (Accessed 20/12/2014). In another phishing case, ten individuals were extradited from Romania, with another nine sought: http://www.fbi.gov/newhaven/press-releases/2012/connecticut-federal-jury-finds-romanian-national-guilty-of-participating-in-internet-phishing-scheme (Accessed 20/12/2014). The US is actively seeking information in relation to the location of numerous foreign defendants for malware distribution, such as Bjorn Daniel Sundin and Shaileshkumar Jain, who are sought in relation their role with a scareware website, which purportedly caused losses to Internet users in 60 countries. See http://www.fbi.gov/chicago/press-releases/2010/cg052710-1.htm (Accessed 20/12/2014). In the Coreflood Botnet case, a complaint was also filed against thirteen 'John Does', without knowing where these individuals were located: *USA v John Doe* (Connecticut Complaint, 11 April, 2011), [20].

[169] *Usman Ahzaz, supra* note 147. See also, for example, the Stubhub indictments and extraditions, where it was said "[t]oday's arrests and indictment connect *a global network* of hackers, identity thieves and money-launderers who victimized countless individuals in New York *and elsewhere*" (emphasis added). See http://manhattanda.org/press-release/da-vance-city-london-police-royal-canadian-mounted-police-announce-arrests-and-crimina (Accessed 20/12/2014).

[170] See e.g. *USA v Ovidiu-Ionut Nicola-Roman and others* (District of Connecticut Indictment, No. 3:07-Cr-12-JCH, 18 January 2007), [23], *USA v. Ciprian Dumitru Tudor and others*

mentioned in the indictment, it can only be a fraction of those affected across elsewhere.[171]

Similarly, the ease of mass distribution of content has meant that extraditions can be sought once any customers of illegal content are located in the US. Maksym Shynkarenko, a Ukrainian national, was extradited to the US from Thailand, where he was on vacation, for numerous child pornography offences (**the Shynkarenko extradition**). The charges were based on his alleged involvement with various for-profit child sexual abuse websites, which had been operated from the Ukraine and other locations (but not the US).[172] Jurisdiction in this case was primarily based on the fact that individuals in New Jersey purchased content from their websites,[173] the transportation of the content to those individuals,[174] and simply the availability of the content in New Jersey.[175] However, the object of the enterprise, as the indictment acknowledges, was to "operate Internet websites containing images and videos of child pornography and sell access to these websites *to customers around the world*."[176]

The above examples dispel the aforementioned assumptions by Brenner and this like regarding the limitations of enforcement jurisdiction in the cybercrime environment,[177] and are demonstrative of the ability of States to harness the malleability of territoriality, which I highlighted in chapter five, in their

---

(District of Connecticut Indictment, No. 3:07-Cr-12-JCH 10th November 2010), [17], and *US v Evgeniy Bogachev* (No. 14-127, May 19 2014), [24].

[171] See e.g. the extradition of Deniss Čalovskis to the USA from Latvia for his role in creating the Gozi virus. The indictment recognised that over a million computers were affected worldwide, and pointed to approximately 17,000 being in the US: *USA v Deniss Čalovskis* (New York Indictment, S4 12 Cr. 487, January 23 2013), [3]. Other conspirators, from various jurisdictions, have already been arrested. See the cases of Nikita Kuzmin and Mihai Ionut Paunescu. Čalovskis' case is currently before the ECtHRs: *Čalovskis v Latvia* (no. 22205/13, 24 July 2014).

[172] *USA v Maksym Shynkarenko* (New Jersey indictment, Crim No. 08-625-WHW, 16 September 2008), [4] of count one.

[173] Ibid, [4] & [11] of count one.

[174] Ibid, counts two through seventeen.

[175] Ibid, [3] of count eighteen.

[176] Ibid, [3] of count one. Emphasis added. There were approximately 560 consumers of the content, based in 47 US states, but this figure may well have been dwarfed by the number of consumers in other countries.

[177] See *supra* section 7.2. Statements such as the following by Finklea (2012), 10, are particularly discredited: "[w]hile criminals may operate across jurisdictional boundaries, law enforcement cannot … For a given crime, federal law enforcement may be able to pursue an investigation provided that the criminal act, criminal actors, and victims are all within the United States."

cybercrime prosecutions. Prior to the Internet era, many States were "wary of the increasingly extraterritorial drift of U.S. criminal statutes"[178] in the extradition context, but the new drift is territorial. It has never been so easy for a State to claim that a crime has been committed in its territory, whether it is the substantive offence or, as is now common in these cybercrime cases, inchoate offences, such as conspiracy. These acts span the spectrum: accessibility of a site in the US (the O'Dwyer and Shynkarenko extraditions), utilising payment services based there (the Dotcom extradition), communications passing through US computers (*Bendelladj*), storing of information on US servers (the Dotcom and Ahmad and Ahsan extraditions, *Kolarov*, *Bendelladj*) targeting US-based corporations or computers (*McKinnon*, *USA v Sergei Tšurikov*[179]), and any number of victims (the Ahzaz extradition, *Bendelladj*) or consumers of content on foreign operated and hosted sites (the Shynkarenko extradition), being based in the US.

This is not to say that the US was not a proper forum in some of these cases, or that the US did not have strong territorial grounds in others.[180] However, the above demonstrates that the diversity of mechanisms for claiming territorial jurisdiction facilitates the pursuit of extradition even in cases where the jurisdictional case is built on much more unstable grounds.[181] The US itself is well accustomed to the difficulties which concurrency can cause in extradition cases, but as Bassiouni has long ago observed in the extradition context:

> it seems clear that judicial decisions are guided by the interest displayed by prosecuting authorities and reject the claims of defendants whenever the state having concurrent or alternative jurisdiction does not challenge the jurisdiction of the requesting state.[182]

---

[178] Nadelmann (1993), 413.
[179] *Supra* note 162.
[180] E.g. in the phishing cases, noted *supra* notes 168 and 170 above, some of the banks targeted were American.
[181] E.g. in *O'Dwyer* or the *Regpay* case. Sansom (2009), 225 claims that "Regpay manifested the intent of engaging in business or other interactions within the United States, and as such, American jurisdiction was proper." However, since a substantial portion of hosting providers are located in first world countries, particularly the US, serious questions must be asked of such jurisdictional assertions. The issue of which jurisdiction should prosecute an offence becomes dependent on factors such as where the hosting providers with the cheapest services are based, and it allows the US to claim jurisdiction over content which may not even have been consumed by Americans.
[182] Bassiouni (1974), 221.

This previous experience has possibly contributed to, and emboldened, current extradition practices by US authorities, and the above supports the view that the recent evolution of extradition structures, particularly when coupled with the malleability of territoriality over cybercrime, "could well be compared to the development of an ever more powerful and efficient vacuum cleaner."[183]

7.5.3. Finger Pointing and Contributory Causes

As mentioned, some of the UK extradition cases (such as the McKinnon and O'Dwyer extraditions) created significant political problems for the government.[184] The fact that there was jurisdictional concurrency, meaning these individuals could also have been prosecuted domestically, but faced trial, sentence (which was potentially much higher in the US in some cases[185]) and incarceration on the other side of the Atlantic, generated considerable public sympathy for the defendants. A blame campaign began, and more often than not, it was the US-UK Extradition Treaty 2003 that was pointed to, with strong media portrayals that it was imbalanced and heavily weighted in favour of the US. Even parliamentary reports pointed the finger in this direction.[186] However, an analysis of this Treaty shows that any imbalances in obligations were not a contributory cause for the difficulties which emerged between the US and the UK.[187]

---

[183] Nadelmann (1993), 459.
[184] See section 7.3.
[185] The prospect of McKinnon facing seventy years in prison was referred to repeatedly in comments on his case: http://www.dailymail.co.uk/news/article-1158173/Pentagon-hacker-faces-70-years-US-jail--CPS-wont-try-Britain.html (Accessed 20/12/2014).
[186] Home Affairs Committee, 'The US-UK Extradition Treaty' (20th report of Session 2010-2012, HC 644, 30 March 2012), [21], and Joint Committee on Human Rights, 'The Human Rights Implications of UK Extradition Policy' (15th Report, HL 156, HC 767, 22 June 2011), [192]. See also Sir Menzie Campbell's review: http://www.guardian.co.uk/world/2012/sep/16/gary-mckinnon-extradition-lib-dems (Accessed 20/12/2014).
[187] One of the questions the government asked the authors of the Baker Review to consider was whether the US-UK Extradition Treaty was balanced. The sticking point in the Treaty is Article 8(3)(c) which requires UK extradition requests to the US to meet a certain evidential threshold, with no reciprocal requirement for US requests to the UK. What seems to have been missed by many, however, is that the reason why there is there is no reciprocal obligation is because of the loosening of the *prima facie* evidential requirement in UK extradition law; over forty other countries have been designated by the Home Secretary as not having to meet this evidential threshold. (See e.g. the EA 2003 (Designation of Part 2 territories) (Order 2003 SI 2003/334.)) The Baker Review (2011), *supra* note 37, 1.20 concluded that the Treaty did "*not operate* in an unbalanced manner" pointing to the respective evidential thresholds for seeking an arrest warrant (a crucial stage in any extradition) in both countries, which they saw as

More to the point were claims that these cases demonstrated "exorbitant extraterritorial jurisdiction"[188] and the "overzealousness of US prosecutors."[189] The former, however, has mischaracterised the jurisdictional ground relied upon: as the above analysis of cases demonstrates, the US rarely needs to rely on extraterritorial jurisdiction, given the breadth of territoriality. Moreover, the US is not alone in interpreting territorial jurisdiction in the ways identified above. Given my findings in chapter five, there is limited scope for solely critiquing US practices here, since the same interpretations of territoriality have been recognised in UK cases, and some are even being promoted through EU harmonisation initiatives.[190] Prosecutorial aggression was also certainly a key factor in these cases, and typified in cases like the O'Dwyer extradition, where it was not even clear that he had committed an offence in the UK[191] or the US.[192] Nevertheless, US LEAs are keen to deter all forms of cybercrime, and statements such as those with which I introduced this chapter follow each extradition.[193] And there is at least some evidence that it is bearing fruit. As one of Sweden's most successful carders told Misha Glenny:

> I never use American credit or debit cards … because that would put me under the legal jurisdiction of the United States wherever I am on the planet. So I just

---

essentially equivalent (ibid, 7.42). However, they did not directly answer the question asked of them; they focused on whether domestic extradition procedures in both countries indirectly result in parity of obligations, rather than on the specific question of whether the Treaty itself is balanced (which it is not, given the lack of reciprocal requirement). This could be seen as slightly disingenuous, but regardless of one's perspective on Article 8(3)(c), it is certainly not a *cause* of these 'problematic' cybercrime extraditions. My review of the affidavits supporting many of the above extradition requests suggest that US requests are normally very well supported, and would even meet a *prima facie* evidence threshold. See also Baker Review (2011), *supra* note 37, 235, footnote 14.

[188] Home Affairs Committee, *supra* note 186, para. 30, quoting Julian Knowles, Matrix Chambers.

[189] Ibid.

[190] See e.g. Article 9(2)(b) Framework Decision on Racism and Xenophobia (2008/913/JHA of 28 November 2008), which requires Member States to ensure that territorial jurisdiction will extend to hosting unlawful material on their territories.

[191] Existing authority in the UK at the time suggested that O'Dwyer had not committed an offence. See discussion of the *Rock v Overton* case in chapter five, section 5.2.3.1.

[192] See e.g. *Flava Works Inc. v Marques Rondale Gunter* (US Court of Appeals, 7th Circuit, no. 11-3190, 2nd August 2012).

[193] See e.g. Peter Edge, Homeland Security Investigations Executive Director: 'Cyberspace affords no refuge from American justice' (http://www.justice.gov/opa/pr/member-organized-cybercrime-ring-responsible-50-million-online-identity-theft-sentenced-115 (Accessed 20/12/2014)) and US Attorney Fishman: "[t]his extradition shows that hiding behind computers and borders does not deter us." (http://www.justice.gov/usao/nj/Press/files/Kolarov,%20Aleksi%20Extradition%20PR.html (Accessed 20/12/2014)).

> do European and Canadian cards, and I feel both happy and safe with that – they will never catch me.[194]

Other obvious contributory factors to the US's ability to extradite in these cases were the domestic changes made to extradition structures, which facilitated extradition even in cases of concurrency,[195] and the investigative powers of the US, which are undoubtedly enhanced by the density of Internet infrastructure there.[196] Less obvious, however, was the role of TGNs. In the Ahsan extradition, one of the judicial review actions concerned the failure of the DPP to take into account the UK/US Agreement, which contains guidance agreed between the Attorney Generals of both countries, in his decision not to prosecute.[197] This required, *inter alia,* an early sharing of information between prosecutors, and consultation in cases of concurrent jurisdiction.[198] This did not occur in the Ahsan extradition, and the court did not find issue with the DPP's lack of consideration of the UK/US Agreement, because that Agreement "does not require consideration to be given to the prosecution of a requested person in this country in circumstances where there has been no investigation of his case in this country."[199] Therefore, the lack of a domestic police investigation[200] prevented the issue of forum from being discussed in one of the only forums where it could have been at the time (i.e. between prosecutors). In fact, due to the "Chinese Wall" [201] that exists between CPS prosecutors considering domestic prosecutions and CPS lawyers acting for foreign countries in extradition cases, the lack of investigation means the former group may not even be aware that a particular extradition is proceeding.

---

[194] Glenny (2011), 4.
[195] See section 7.4 above.
[196] It was information provided by many US based service providers that resulted in the identification of many of the individuals in these cybercrime extradition cases. See e.g. the O'Dwyer extradition, in particular *Reh* affidavit, *supra* note 132, [15], and *Di Laura* complaint, *supra* note 131, [22]-[27]. See further chapter four.
[197] See discussion of the UK/US Agreement in chapter six, section 6.2. Unlike countries like Germany, there is no police duty to investigate cases when informed of criminality.
[198] Ibid, [4].
[199] *Ahsan* [2008] EWHC 666, [36]. See relatedly *McKinnon* [2009] EWHC 2021, [55].
[200] Unlike countries like Germany, there is no police duty to investigate cases when informed of criminality.
[201] CPS Statement, 'Case update on the extradition of Babar Ahmad', (6th August 2012), available at: http://www.cps.gov.uk/your_cps/our_organisation/babar_ahmad.html (Accessed 20/12/2014).

A related contributing factor is the impact which MLA can have on the outcome of extradition cases. According to the High Court, the purported reason for non-prosecution in the Ahmad and Ahsan extraditions was because:

> the necessary evidence was not available to the police in this country to link Babar Ahmad and Talha Ahsan to the websites and the other material matters. That information, being available in the United States as the ISPs were based there, enabled the US Prosecutor to put forward the necessary linking evidence.[202]

One must ask *why* the CPS apparently had insufficient evidence to prosecute[203]. Caroline Lucas MP claimed that it was because "[t]he bulk of the evidence was shipped straight to the US by the police."[204] An analysis of the Criminal Complaint against Ahmad[205] suggests that this was an accurate assertion; the majority of the evidence relied upon in the Complaint was evidence from the UK, including hard drives and floppy discs taken from Ahmad's office.[206] Moreover, the High Court certainly misstated the case when they said the ISPs were all based in the US, as one of the key pieces of evidence relied upon in the Complaint was information from Netscalibur, Ahmad's access provider in the UK.[207]

This seems to be a case of having one's cake and eating it. In the McKinnon extradition, one of the biggest barriers to a domestic trial was said to have been the difficulty of getting physical evidence from the US to the UK. In the Ahmad extradition, it would seem to have been easier to pass the intelligence and the information from the US-based hosting provider to UK LEAs, rather than the transferral of evidence from the UK to the US. But it is not uncommon to overstate the difficulties in moving evidence to facilitate the extradition of a person to a requesting State that has initiated the investigation. This must not be exaggerated in the 21st century. As one court has stated: "[i]n the year 2011, it is difficult to conceive that the prosecution could have difficulty in moving

---

[202] *Hamza and others* [2012] EWHC 2736, [205].
[203] And it is not clear that they did. The CPS claimed to have only received a "small number of documents" from the Met in relation to Ahmad. CPS statement on Ahmad, *supra* note 201. The High Court, however, said that the CPS had considered 32 "significant exhibits." *Hamza,* ibid, [151].
[204] http://www.bbc.co.uk/news/uk-politics-15882911 (Accessed 20/12/2014).
[205] *USA v Ahmad* (Criminal Complaint of Special Agent Craig Dowling, 28 July 2004),
[206] Ibid, [32].
[207] Ibid, [12].

its evidence from one jurisdiction to another."[208] The greater difficulty is normally for the defendant to prove his case and support it with witnesses, if he is extradited from his home country.[209]

What is clear is that the prior movement of evidence pursuant to MLA obligations can directly impact on any subsequent decisions on domestic prosecutions.[210] The above also demonstrates how the work of TGNs (or lack thereof) at the investigative stage can have a huge bearing on whether individuals are ultimately extradited and where they face trial. As I have noted,[211] TGNs can be "opaque venues for the exercise of unfair and inequitable power"[212] where powerful States can coerce other actors to secure preferred outcomes,[213] prioritising domestic concerns,[214] over other potential outcomes. Police in a requesting country may be under-resourced, or lacking expertise in the investigative techniques required, and may be only too happy to "free ride",[215] on the prosecutorial willingness of a foreign partner.

From an enforcement perspective this may not appear to be of importance: what matters is not who prosecutes, but that it is done. However, the UK experience demonstrates the political potency which can accumulate around these extraditions, which may prompt States to revert to constructs like nationality bars. Indeed, the UK introduced an extradition bar directly as a result of the US cybercrime extradition requests, but it did not opt for a nationality bar, given its historical aversion to this device. Instead, it introduced a forum bar, which continues to allow determination between TGNs to assume priority on place of prosecution. This will be explained in my final section below.

---

[208] *Steve Ferguson, Ishwar Galbaransingh v The Attorney General of Trinidad and Tobago* (CV 2010-04144, 7 November 2011), [86].
[209] Ibid. [88]
[210] This was also an issue in the Dotcom extradition. New Zealand police provided cloned hard drives to the FBI even in breach of domestic law, as the items should have remained in the control of the Commissioner of Police according to a direction given by the Solicitor-General under s.49(2) of the Mutual Assistance in Criminal Matters Act 1992. See *Dotcom v Attorney General* [2013] NZHC 1269 (31 May 2013), [8(d)].
[211] See chapter four, section 4.4.
[212] Newman and Zaring (2013), 255.
[213] Verdier (2009), 130.
[214] Ibid, 126.
[215] Eilstrup-Sangiovanni (2009), 202.

7.6 Forum Bars

By late September 2012 Theresa May must have been growing weary of US cybercrime extraditions. She had sat on the McKinnon extradition for two years, and long standing cases like Talha Ahsan's were generating similar headaches, with the latter also having been diagnosed with Asperger's Syndrome. Ahsan and Ahmad had also already cost the State in the region of millions of pounds, having been detained in high security facilities without trial for five and eight years respectively, the latter being longest pre-trial detention in the British history.[216] In the interim, cases like that of O'Dwyer had also arisen. The number of demonstrations[217] and e-petitions,[218] and ink spent on articles about the cases, was growing by the day. A radical overhaul of extradition practices was deemed necessary and May moved decisively on the 16th of October 2013 to ensure that she would never be placed in this position again.[219] First, she bowed to political pressure and announced McKinnon would not be extradited due to human rights concerns.[220] Second, she would also, as discussed above, remove her ability to review human rights considerations after the end of the statutory appeal process, with only the High Court able to review such issues in the most exceptional of cases.[221] This maps directly onto the trend of the executive disempowering itself, with the judiciary being passed the buck, with tightly cabined discretion. Third, she announced that the UK/US Agreement would be updated, and the creation of new Guidelines from the DPP on dealing with cases of concurrency. Most importantly, however, she also announced that the UK would introduce a

---

[216] http://www.guardian.co.uk/commentisfree/2012/oct/04/babar-ahmad-extradition (Accessed 20/12/2014).
[217] http://www.demotix.com/news/1502676/protest-against-extradition-syed-talha-ahsan-and-babar-ahmad#media-1502670 (Accessed 20/12/2014) and http://news.bbc.co.uk/1/hi/uk/8223734.stm (Accessed 20/12/2014).
[218] http://epetitions.direct.gov.uk/petitions/885 (Accessed 20/12/2014) and http://www.change.org/en-GB/petitions/ukhomeoffice-stop-the-extradition-of-richard-o-dwyer-to-the-usa-saverichard (Accessed 20/12/2014).
[219] https://www.gov.uk/government/news/theresa-may-statement-on-gary-mckinnon-extradition (Accessed 20/12/2014).
[220] This was despite the numerous previous decisions to the contrary, and the fact that it patently contradicted her own decision in the Ahsan extradition, a little over a week later.
[221] See now s.108(7) EA 2003, introduced by s.50, and Sch. 20, Part 2, para. 12 Crime and Courts Act 2013. For critique see Justice 'Crime and Courts Bill 2012: Briefing for Report Stage' (March 2013), paras. 38-41.

new[222] forum bar for extradition cases, contrary to the direct recommendations of the Baker Review, which thought a forum bar would, *inter alia,* involve scrutiny of domestic prosecutorial decisions and increase the complexity and length of extraditions.[223]

The fact that this was a response to various public outcries was plain to be seen: "[t]he introduction of a forum bar to extradition responds to the widespread concern in Parliament, and amongst the public, that insufficient safeguards are currently built into cases of concurrent jurisdiction."[224] And the public had little time to wait for this to be 'improved.' On the 14th of January 2013 it was announced that the forum bar would be introduced through the Crime and Courts Bill,[225] and the amendments were published on the 5th of February 2013.[226] But since that Bill was already at the end of the legislative process by that point, neither Houses of Parliament had much time to consider the proposals, which was staunchly criticised in both arenas.[227]

When broken down, the forum bar, for both category one and two territories, essentially allows a judge to refuse extradition if he decides it would be in the interests of justice to do so.[228] There is first a threshold consideration, that a substantial measure of D's relevant activity must have been committed in the UK. If this is satisfied, the court must then consider seven specified matters related to the interests of justice. These factors (paraphrased) are: the place where most of the loss or harm occurred, the interests of any victims, the views of prosecutors that the UK is not the appropriate jurisdiction to prosecute the

---

[222] A forum bar was on the statute books in ss.19B and 83A EA 2003, introduced by the Police and Justice Act 2006, but never brought into force.
[223] Baker Review (2011), *supra* note 37, pages 205-230.
[224] Crime and Courts Bill, 'Supplementary Memorandum submitted by the Home Office', (C&C 15, 7th Feb 2013).
[225] Hansard 14 January 2013: Column 642-643.
[226] House of Commons, Notice of Amendments, (5th Feb 2013), Crime and Courts Bill Committee 109-08, Public Bill Committee.
[227] Lord Lloyd in the Lords said "They have been brought before us at the last moment, and it is almost disgraceful for us to be asked to amend the law in an important respect that will undoubtedly affect our foreign relations without the matter having been properly considered in this House and the other places." (Hansard 25 March 2013: Column 806). See also the comments of Lord Rosser (Hansard 25 March 2013: Column 901) Lord Dubs (Hansard 25 March 2013: Column 896), and David Hanson in the Public Bills Committee (Hansard 12 February 2013: Column 417).
[228] See ss.19B and 83A EA 2003, inserted by s.50 and Sch. 20, Part 1 Crime and Courts Act 2013.

case, whether evidence could be made available for a domestic trial, any delay that might result from proceeding in one jurisdiction over another, the desirability and practicability of all prosecutions relation to the extradition offence, and D's connections with the United Kingdom. While the exhaustive nature of the list has been criticised for unduly fettering judicial discretion,[229] this is, as mentioned, nothing new when power is transferred to the judiciary in matters pertaining to extradition. Moreover, the specific factors here are relatively broad and, considering that the first limb entails considering whether a "substantial measure" of the relevant activities occurred in the UK, there is ample legroom for judicial interpretation as issues arise in practice. The final specified matter, (D's connections with the UK), indirectly requires consideration of nationality and residence in forum decisions, which finally takes account of these matters in UK extradition law, without constituting a blunt bar with which the above-mentioned report by Cockburn CJ had so many concerns.[230]

The UK's forum bar has significant potential for the judicial development of understandings of territoriality,[231] particularly in the realm of cybercrime, and will serve to embed reasonableness amongst transgovernmental networks, as actors will be more cautious before requesting extradition knowing that the question of forum will be addressed by the judiciary. Indeed, we are already seeing a jurisprudence develop in this regard.[232]

However, there is one completely novel feature of the new forum bar, which has been called the prosecutorial "veto."[233] Prosecutors can issue a certificate[234]

---

[229] Justice 'Crime and Courts Bill 2012: Briefing for Report Stage' (March 2013), [31].
[230] See *supra* note 77.
[231] This has been sorely lacking in the extradition context because, as has been discussed above (section 7.4), the process developed so as to preclude such analysis. Some examples of cases from other jurisdictions, however, include: *USA v Cotroni* [1989] 1 SCR 1469, and *Steve Ferguson, Ishwar Galbaransingh v The Attorney General of Trinidad and Tobago* (CV 2010-04144, 7 November 2011). In the former case, La Forest J listed a range of factors to be considered when deciding on whether to extradite or prosecute locally. The latter case epitomises US prosecutorial aggression; extradition was sought despite the defendants being prosecuted locally on corruption charges, which were committed in Trinidad and Tobago. The US's jurisdictional claim essentially lay in the fact that proceeds from the allegedly fraudulent activity ended up in US banks. Ibid, 20.
[232] *Dibden v Tribunal De Garde Instance De Lille France* [2014] EWHC 3074 and *Piotrowicz v Regional Court in Gdansk Poland* [2014] EWHC 3884.
[233] Lord Rosser, (Hansard 25 March 2013: Column 891).

which operates to prevent judicial consideration of forum if a prosecutor certifies that he has considered domestic prosecution, and decided there are corresponding offences which could be charged, and either:

- the prosecutor makes a 'formal' decision not to prosecute because there would be insufficient evidence available, or because prosecution would not be in the public interest, or

- the prosecutor makes a decision not to prosecute because of concerns with the disclosure of sensitive material (e.g. relating to national security, international relations, or the prevention of crime).

When a Home Office Minister was questioned in the House of Lords as to the purpose of this prosecutorial veto system, he responded: "the purpose of the forum bar is to ensure that prosecutors give due consideration to whether a prosecution should take place in the UK. That does not always happen at the moment."[235]

The Lords would have had to have been well-enough tuned into discussions to have realised that Lord Taylor completely dodged the relevant question here. He was asked about the purpose of the prosecutorial certificates, not the purpose of the forum bar. And if the purpose of the certificates is that which he alleges above, one must question why they didn't simply impose an obligation on the CPS to consider domestic prosecution in every extradition case where there was jurisdictional concurrency.

A closer look at the historical record, however, reveals the true purpose behind the system. Another Home Office Minister, a month previously, had been more frank about what the prosecutorial veto was tackling:

> We do not want the judge considering forum to cause any undesirable consequences, for example jeopardising a possible investigation and/or prosecution in the requesting state by ordering the disclosure of sensitive foreign material.[236]

Considering that judges, in deciding on forum, must already bear in mind the views of prosecutors and the availability of evidence, and are well accustomed to dealing with Public Interest Immunity arguments, this mistrust of the

[234] See (as inserted) s.19C-F, and s. 83B-E EA 2003.
[235] Lord Taylor (Hansard 25 Mar 2013: Column 899).
[236] Jeremy Browne (Hansard, Public Bills Committee, 12 February 2013, Col 413).

judiciary is striking. The forum bar, as enacted, demonstrates a strange tension between on the one hand, empowering the judiciary to deal with issues of jurisdictional concurrency (but as *per* the trend, in a highly cabined way), so as to make forum decisions "more open and transparent",[237] but on the other hand, building in a mechanism by which these issues may be kept from ever seeing the light of day. As Justice has commented: "…it allows for a forum shopping agreement between the countries' prosecuting authorities made behind closed doors." [238] This is certainly new ground in the balancing act between maintaining discretion, and ensuring flexibility and the credibility of extradition commitments. A new character is recognised and introduced into the traditional extradition equation: the prosecutor. For too long it has been thought that it is only national courts and executives that are involved in resolving concurrent jurisdiction cases in the extradition process,[239] but the creation of prosecutorial certificates is recognition of the role of prosecutors, and of TGNs, in these determinations. The government sought to build in a mechanism to ensure pragmatic prosecutorial-oriented decision-making could assume priority over forum determinations by the courts. While there are concerns and questions as to why these issues were removed from the courts, at least in the UK prosecutors must now consider domestic guidance on forum,[240] and their decision to issue a prosecutorial certificate is subject to judicial review.[241] It is likely to be a novel creation, not found in other jurisdictions, but it highlights the role of TGNs in resolving cases of jurisdictional concurrency. Their role, and constructs like the forum bar, ought to be of wider interest in the suppression project, to which I will return in my concluding chapter.

[237] Lord Taylor (Hansard 25 Mar 2013: Column 888).
[238] Justice 'Crime and Courts Bill 2012: Briefing for Report Stage' (March 2013), para. 34.
[239] Abelson (2009), 5 for example, states "the task of resolving concurrent exercises of criminal jurisdiction will remain with national courts and executives."
[240] This guidance must also be considered prior to issuing a prosecutorial certificate: *Dibden v Tribunal De Garde Instance De Lille France* [2014] EWHC 3074, [20].
[241] The decision of the prosecutor is judicially reviewed under ss.19E or 83D EA 2003. This is not to say, however, that forum arguments will have received equivalent attention as if the courts had considered the issue under ss.19B and 83A EA 2003, as judicial review proceedings are limited to challenges based on issues of unreasonableness, *ultra vires,* etc.

7.7 Conclusion

This chapter has traced aspects of the history of UK extradition law, and demonstrated the forces which led to recent structures. From the perspective of jurisdictional concurrency, these structures were characterised as having broadly prioritised the enhancement of binding obligations and improvement of international cooperation in the movement of suspected criminals—of course a laudable goal—at the expense of maintaining discretionary powers of refusal in extradition proceedings. The harmonisation of substantive criminal laws in conventions like the Cybercrime Convention is a crucial driver behind this objective, as it eradicates difficulties like double criminality, which had long plagued extradition law, and facilitates extraditions where bilateral treaties do not exist. It is a process which invites efficiency, speed, and simplicity. It invites treating cybercrime just like every other crime that the international community is accustomed to dealing with in transnational crime conventions. But the UK extradition experience militates against such a *laissez faire* approach. The UK experience demonstrates the political potency of these extraditions, particularly in cases of concurrent jurisdiction, and when British nationals are involved. It demonstrates how the pursuit of cooperation in extradition legislation can result in the space for consideration of the normative issues arising being lost in a complex web of legal bureaucracy and opaque networking between TGNs.

Despite focusing almost exclusively on extradition requests from the US, I also sought in this chapter to stress that this must not, as has been commonly assumed, be treated as an isolated problem between the UK and the US, which eventuated only because of their bilateral extradition treaty. Many other countries are receiving similar requests, and the conditions facilitating such extraditions—which created difficulties in the UK—are undoubtedly also present elsewhere. Moreover, as the enforcement and investigative tools of States increase through harmonisation initiatives,[242] the platform is set for other countries to also begin utilising extradition more heavily. We live in a time where it has never been easier for a foreign suspect to be identified, investigated, and an extradition case built, without the investigator ever leaving

[242] See chapter four.

his desk. While jurisdictional concurrency has long caused problems for States in extradition proceedings, the ease of characterising cybercrime activities as territorial offences means this issue has become a much more pronounced problem in this realm.

In contradiction to Brenner, it is clear that extradition is used in cybercrime cases, both to incapacitate criminals whose acts impact on the US, and as part of a powerful deterrence campaign. It is one of the key tools in the ""colonization" of the global Internet"[243] by the US. All of the cybercrime cases addressed above involved jurisdictional concurrency, and some, such as the O'Dwyer extradition, were striking for the tenuousness of the jurisdictional claim, and for extradition being sought from a law enforcement ally that would have been well equipped to prosecute the case itself. There are numerous reasons why US LEAs have demonstrated themselves to be somewhat dogmatic in their unilateral pursuit of cybercrime extraditions: their LEAs may be under domestic pressures to demonstrate the fruits of their investigative work,[244] and they may also lack faith in the capacities of some foreign justice systems and abilities to manage complex cybercrime prosecutions.

From an enforcement perspective the preparedness of the US to pursue costly extraditions against criminals whose acts may be impacting countries across the world may be lauded. Indeed, it may cause widespread relief. However, it also brings numerous concerns. There are concerns for defendants, who may find it more difficult to defend themselves in a foreign country, or find themselves incarcerated far from family and friends, simply because, for example, an aspect of his criminality passes through the infrastructure of a foreign country. Such an outcome appears patently unfair.[245] Nevertheless, the malleable nature of territoriality invites and obscures the unreasonableness of

[243] Amsterdam and Rothken (2013), 29.
[244] As Verdier (2009), 126 notes, networks may ignore globally optimal outcomes by prioritising domestic concerns.
[245] Therefore, Beccaria's words continue to be of relevance: "[w]hether it be useful that nations should mutually deliver up their criminals? Although the certainty of there being no part of the earth where crimes are not punished, may be a means of preventing them, I shall not pretend to determine this question, until laws more conformable to the necessities, and rights of humanity, and until milder punishments, and the abolition of the arbitrary power of opinion, shall afford security to virtue and innocence when oppressed." (See Farrar (1880), chapter 35, 'Of Sanctuaries').

such assertions. There is also the concern that when cases like *McKinnon* become political hot potatoes for a State, there is a danger that the State will become uncooperative, reverting to constructs like nationality bars. The UK, for example, was prompted to introduce an extradition bar directly as a result of the cybercrime extradition requests which it received from the US, although this particular bar holds more potential for building jurisdictional reasonableness into the operations of TGNs.

A broader concern is that the ease of extradition will jeopardise one of the key goals of the suppression project: domestic suppression of cybercrime. States have no incentive to build their capacities for cybercrime investigations if they can simply externalise the cost of prosecutions. This is one of the main reasons why UK LEAs have a markedly different approach to cybercrime extraditions, as compared to their US counterparts. As one cybercrime investigator from SOCA stated in an interview:

> [t]here isn't an appetite from the UK to start extraditing people to the UK, unless there was a compelling reason and that was a decision that the prosecutor wished, for example, to complete a case … SOCA's cyber work is very much along the lines of raising capacity and capability in other jurisdictions, and looking at their legislative framework, to ensure they've got the legal means.[246]

In another interview, S1 illustrated the point with a practical example, involving a romance fraud originating from Ghana with some victims based in the UK. The "short term solution"[247] was to seek the extradition of the suspects, but the decision was made to assist in a local prosecution instead. It was said to have been a "nightmare from start to finish"[248] due, in particular, to a Ghanaian law requiring victims to be in physical attendance during the prosecution. This meant a number of UK witnesses had to travel to Ghana for the prosecution, and there were reportedly frequent delays and problems with the prosecution. S1 nevertheless spoke of the utility of the exercise. Extradition, he said, is often not a long term solution, and the question is whether domestic investigators and prosecutors can be strategic in the particular case: "[f]rom an operational point of view, we tried to take the line that complete dependency doesn't give Ghana any motivation to develop their own system. So what we

[246] SOCA Interviewee (3).
[247] SOCA Interviewee (1).
[248] Ibid.

have to do instead is to work with them."[249] Attitudes like this between TGNs would undoubtedly go far towards reducing the problems and tensions arising from jurisdictional concurrency, and I will address some of the tools that could be used to further incentivise such cooperation in my conclusion.

[249] Ibid.

Chapter 8: *Ne Bis in Idem*

8.1 Introduction

Anyone who has watched their share of legal thriller films will know that there are certain rules that prevent re-prosecuting an individual for the same offence. In the US, this is referred to as 'double jeopardy' protection, in other common law jurisdictions, the plea of *autrefois acquit, autrefois convict,*[1] but more commonly in the doctrine and in continental European legal systems, it is known as the *ne bis in idem* principle.[2] This principle has been described as "a fundamental principle of law, which restricts the possibility of a defendant being prosecuted repeatedly on the basis of the same offence, act, or facts."[3] Many authoritative authors consider it to constitute customary international law, at least in relation to trials within the same State.[4]

In 1999, Stessens and Van den Wyngaert claimed that "[a]n international *non bis in idem* principle constitutes an essential guarantee for an individual facing criminal charges in a world which is increasingly internationalised",[5] and that the time was ripe for the international community to adopt a more comprehensive and detailed concept of same. These words ring through more than ever but they have not been heeded, particularly in suppression conventions,[6] and there is nothing on the horizon to suggest that they will be in

[1] See Hooper and Ormerod (2010), 1546-1551.
[2] In some texts, it is called the '*non bis in idem*' principle. For an explanation as to why, from the perspective of Latin semantics and grammar, the phrase *'ne bis in idem*' is preferable, see Bernard (2011), fn1. It literally translates as 'not twice in the same.'
[3] Bockel (2010), 2. For a history of the principle, see Sigler (1963).
[4] Cassesse (2003), 319.
[5] Stessens and Wyngaert (1999), 803-4.
[6] The Harvard Research (1935) Draft Convention on Jurisdiction did contain a provision concerning *ne bis in idem*. Article 13 stated "[i]n exercising jurisdiction under this Convention, no State shall prosecute or punish an alien after it is proved that the alien has been prosecuted in another State for a crime requiring proof of substantially the same acts or omissions and has been acquitted on the merits, or has been convicted and has undergone the penalty imposed, or, having been convicted, has been paroled or pardoned." It is noteworthy that this was only envisaged as applying to aliens, with the commentary making clear that "it would seem inappropriate for a convention on jurisdiction with respect to crime to incorporate limitations on a State's authority over its nationals." Ibid, 613. However, this provision has not found its way into any binding suppression conventions. *Ne bis in idem* provisions are found in the

the near future. Most international human rights instruments actually contain no such protection. Article 4 of Protocol No. 7 to the ECHR (**A4P7**) and Article 14(7) of the United Nations Covenant on Civil and Political Rights only prevent multiple prosecutions within the same State.[7] Some extradition treaties and conventions,[8] on the other hand, can prevent extradition when the individual has previously been prosecuted in the requested State. But these provisions are said not to be generative of any general international law rule providing inter-State *ne bis in idem* protection.[9]

The Cybercrime Convention is unfortunately no exception to this international inclination. Despite the terms of reference of the Committee responsible for drafting the Cybercrime Convention (the PC-CY) specifically requiring consideration of "the problem of ne bis in idem in the case of multiple jurisdictions [attempting to prosecute]"[10] the principle is not mentioned once in the Convention or in its preamble. It is noteworthy that the terms of reference refer to a "problem", rather than a protection, although this is consistent with my conclusions in chapter three that the harmonisation process is a law-enforcement oriented project. The reason for omitting consideration of the principle, however, is not clear. It was hardly an unintentional mistake. In all likelihood, the Committee considered the topic to be too complicated a task with insufficient consensus on its components, and hoped that this aspect of the terms of reference would be quietly forgotten.

As will be seen, not touching on *ne bis in idem* may have been a wise and pragmatic choice by the PC-CY from the perspective of those seeking agreement on an already complex and controversial convention. Yet from the perspective of an individual who may be re-prosecuted for a cybercrime offence in more than one jurisdiction, this omission will be viewed from an altogether different light. In our inter-connected world where individuals can, by the same act, commit offences in numerous countries simultaneously, there

---

Council of Europe's Convention on Offences relating to Cultural Property (ETS no. 119, 1985), but this was only ever signed by six countries and never entered into force.

[7] Article 8(4) of the American Convention on Human Rights is not conclusive—on a literal reading—as to whether it applies between countries. For discussion of these, and other, human rights instruments, see Colangelo (2009), 806-9.

[8] See e.g. Article 9 European Convention on Extradition 1957 (CETS no. 024, 1957).

[9] Colangelo (2009), 809-813.

[10] Para. 11 of the Explanatory Report to the Cybercrime Convention.

is a heightened danger that they could find themselves repeatedly prosecuted by States, which is a fundamental rule of law concern.[11]

The purpose of this chapter is to further problematise jurisdictional concurrency over cybercrime, and to demonstrate both the need, but also the challenges, which will inhere in any attempt to protect individuals from such re-prosecutions. Unlike previous chapters, my concerns over the lack of inter-State protection are not supported by plentiful examples of State practice (in re-prosecuting cybercriminals).[12] However, given the inroads that are being made in investigative enforcement tools,[13] and the numerous cases where States have prosecuted individuals repeatedly for transnational crimes,[14] this discussion is not simply theoretical, but an inevitable and forthcoming practical concern. I begin by considering how one regional initiative (the EU) did develop *ne bis in idem* inter-State protections and analyse the current explanations for this development. I then consider the challenges that would emanate from any attempt to extrapolate the EU framework into a broader international instrument such as a suppression convention: first, I analyse and critique arguments in the literature that States do not need to respect the principle (inter-State) due to their "dual sovereignty";[15] second, I examine what would likely be the most challenging aspect to apply in the realm of

---

[11] Opinion of Advocate General Colomer, Joined Cases C-187/01 and C-385/01 *Gözütok and Brügge* [2003] ECR I-1345, (19 September 2002), [59].

[12] However, there are examples of where cybercriminals have been indicted in more than one country, and where States continue to display an interest in prosecutions, even where one has already occurred elsewhere. Ryan Cleary, for example, was convicted of various computer access offences in the UK in relation to his role with Anonymous and Lulzsec, two infamous hacking groups (see http://content.met.police.uk/News/A-gang-of-hackers-has-been-sentenced-following-a-string-of-highprofile-attacks/1400017318333/1257246741786 (Accessed 20/12/2014)). He was also indicted in the United States in relation to the same acts (*USA v Ryan Cleary (*Indictment, Filed 12th June 2012, CR No. 12-0561). Similarly, Delwyn Savigar, was convicted in the UK of numerous sexual offences as well as possession and distribution of child sexual abuse images (hundreds of thousands of images were found on his computer), but the US maintain an interest in his extradition in relation to his running of a global child pornography bulletin board. See http://www.theguardian.com/society/2010/may/27/child-porn-delwyn-savigar-extradition (Accessed 20/12/2014). Section 80 EA 2003 would bar their extradition if a second prosecution could not occur in the UK for the acts for which they are sought in the US. This would turn on whether the offences for which they are sought are the same, or substantially the same, as the offences for which they have been convicted. For pre-EA 2003 case law on this, see *Connelly v DPP* [1964] AC 1254, at pp. 1310-1328, *per* Lord Morris. This will of course be of no utility if they travel to a third country and are extradited from there.

[13] See chapter four.

[14] See below section 8.4.1.

[15] See below section 8.3.

cybercrime, namely the concept of *idem*. I do this by looking at the nascent jurisprudence of the CJEU and the recent convergence of approaches on the concept of *idem* between this court, and the ECtHRs. Current academic interpretations of this development have the potential to render any potential inter-State protection nugatory when applied to cybercrime. I argue this is a result of a mistaken attempt to imbue the principle of *ne bis in idem* with domestic charging considerations and can therefore be addressed. Cybercrime is fertile ground for difficulties in the application of this principle, but I argue that the current approach of the CJEU affords the most potential for wider development, which will be necessitated as cybercrime enforcement capacities proliferate.

8.2 *Ne Bis in Idem* in the EU

The application of *ne bis in idem* between countries has been long recognised within Europe; prior to the first enlargement of the European Community (**EC**), four of the then six Member States barred prosecution if there had been a previous foreign prosecution.[16] When the UK joined the EC in 1973, this number increased, because the common law had also long recognised the principle applying "whether the previous conviction or acquittal … was by an English court or by a foreign court."[17]

In the sphere of criminal law[18] this protection being afforded between States has its roots in the 1985 Schengen Agreement,[19] which was followed by the Convention Implementing the Schengen Agreement (**CISA**), and there have been numerous other subsequent legal instruments agreed which are

[16] See the opinion of Advocate General Mayras in Case 45/69, *Boehringer v Commission* [1972] ECR 1281, at 1295-6. However, of those four, only the Netherlands applied the principle without reservation; the other three states only recognised it if the principal offence had been committed exclusively abroad. Ibid.

[17] *Treacy v DPP* [1971] AC 537, 562D *per* Lord Diplock. See also *R v Aughet* [1919] 13 Criminal Appeal Reports 101.

[18] The *ne bis in idem* principle has a longer history in Union law, due in particular to the competition field. For an account of this historical trajectory, see the Opinion of Advocate General Colomer, *Gözütok and Brügge*, *supra* note 11, [48] et seq.

[19] In 1987 a 'Convention between the Member States of the European Communities on Double Jeopardy', was also agreed, but it never entered into force as only Italy, France, and Denmark ratified the Convention.

collectively known as the Schengen *acquis*.[20] The 1985 Schengen Agreement and CISA were negotiated outside of EU structures,[21] but a Protocol to both the EU and EC Treaties (now, post Lisbon, Protocol 19 to the Treaty on European Union (**TEU**) and the Treaty on the Functioning of the European Union (**TFEU**)), attached to the Treaty of Amsterdam, incorporated the *acquis* into EU law.[22]

8.2.1. CISA and Article 54

The text of Article 54 of CISA, as currently translated into English,[23] states that:

> [a] person whose trial has been finally disposed of in one Contracting Party may not be prosecuted in another Contracting Party for the same acts provided that, if a penalty has been imposed, it has been enforced, is actually in the process of being enforced or can no longer be enforced under the laws of the sentencing Contracting Party.

This wording is dealt with in more detail below but, *prima facie*, it carves out a significant deviation from the non-recognition of international (inter-State) *ne bis in idem* protection. However, this is itself curtailed by Article 55 of the CISA, which provides the possibility of opt-outs from Article 54 in certain situations, and this provision is heavily relied upon in arguing for the non-recognition of the principle applying between States.[24] In the context of cybercrime, the most pertinent sub-section in Article 55 allows a Contracting Party, "when ratifying, accepting or approving" the CISA, to declare that it is not bound by Article 54:

> …where the acts to which the foreign judgment relates took place in whole or in part on its own territory; in the latter case, however, this exception shall not

[20] The Schengen *acquis* was published in: OJ L/239, 22.09.2000.
[21] This is something that was not appreciated by Colangelo in his 'dual sovereignty' argument: see below, section 8.3.
[22] When the Amsterdam Treaty came into force on 1 May 1999, each element of the *acquis* had to be designated a legal base, which was done by Council Decisions 1999/435/EC and 1999/436/EC of 20 May 1999. The UK has opted-in to the provisions concerning *ne bis in idem*. See Article 1(a)(1) of the consolidated version of Council Decision 2000/365/EC of 29 May 2000 (OJ L 131, 1.6.2000, p. 43), published in Council Notice 2014/C430/01 of 1 December 2014 (OJ C430 57, 1.12.2014).
[23] See OJ L/239, 22.09.2000, which published the Schengen *acquis* as referred to in Article 1(2) of Council Decision 1999/435/EC of 20 May 1999.
[24] Colangelo (2009), 814.

> apply if the acts took place in the territory of the Contracting Party where the judgment was delivered.[25]

In other words, parties are free to declare that they are not bound by Article 54 when the conduct occurred exclusively in its territory, or where part of the criminality occurred on its territory and the party that delivered judgment has not suffered part of the criminality on its territory. A Party cannot opt-out of Article 54 if it, and the Party which delivered judgment, both suffered criminality on their respective territories. In practice, this would render any declaration under Article 55 inapplicable to most cybercrime cases: as previous chapters have shown, cybercrime will rarely occur exclusively within one State's territory, and in the more likely situation where part of the criminality occurs there, it is also likely that some of the acts will have taken place in the first State's territory.

Another reason why Article 55 may not limit the protection afforded under Article 54 is because the unilateral declarations and reservations under Article 55 are arguably no longer legally valid. There is no recent authoritative information available as to the number of declarations, their content, or when they were made,[26] but in a Commission Staff Working Paper, it appears there have been seven declarations under Article 55 issued by the following countries: Austria, Germany, Denmark, Greece, Finland, Sweden, and the UK.[27] While it is implicit in both the Green Paper and the Commission's Staff Working Paper, as well as the most authoritative academic sources on *ne bis in idem*, [28] that existing declarations and reservations continue to apply, Leidenmühler has argued convincingly that unilateral declarations and reservations made pursuant to Article 55 are no longer legally valid, pointing to the absence of such instruments being mentioned in either the annex to the

---

[25] Article 55(1)(a).

[26] I have liaised with numerous senior members of the European Commission and European Council concerning the availability of an authoritative list of Article 55 declarations or reservations. None could locate such information. (Email correspondence with: Clemens Ladenburger, Legal Assistant to the Director General of the Commission's Legal Service; Olivier Tell, Head of Unit DG Justice, European Commission; Thérèse Blanchet, Director, Justice and Home Affairs, Council Legal Service.)

[27] Commission Staff Working Document 'Annex to the Green Paper on Conflicts of Jurisdiction and the Principle of ne bis in idem in Criminal Proceedings' (COM 696 final, 2005), 47.

[28] See e.g. Bockel (2010), 21

Schengen Protocol, or the annexes to the Council decisions concerning the definition of the Schengen *acquis*.[29] Such an interpretation would contradict the position of the European Commission in 2005, an *obiter* comment in a decision of the CJEU,[30] and many of the responses to the Commission's Green Paper which assumed that such declarations continued to be legally valid.[31] Furthermore, it was assumed in the 'Programme of measures to implement the principle of mutual recognition of decisions in criminal matters'[32] that such reservations continued to apply.[33]

Regardless of which interpretation prevails, the number of countries that have made declarations under Article 55(1)(a) of the CISA would appear to be a minority of those to which Article 54 applies. Therefore, although Article 55 does seem to demonstrate a reluctance to sacrifice sovereign rights to punish criminal conduct occurring on Member States' territories, this provision may not, in practice, limit the scope of protection very much. This is due both to the limited role which the exception can play when the criminality has been sustained in both countries concerned, and because of the limited number of countries that have actually made declarations under Article 55. This undermines considerably any arguments that Article 55 significantly dilutes the operation of Article 54 of the CISA.[34]

8.2.2. The FR Charter and Article 50

Article 54 is not the only source of *ne bis in idem* protection in EU law. It has received further protection under the Charter of Fundamental Rights of the European Union (**the FR Charter**). This was proclaimed in Nice in 2000, and was given direct effect by the adoption of the Lisbon Treaty. It applies to the

[29] Leidenmühler (2002), 255.
[30] Case C-491/07 *Turansky* (22 December 2008), [29].
[31] See e.g. the response of the UK Government, which was published in the 40th Report of the House of Lords Select Committee on European Union, at para. 38 of the response.
[32] OJ C/12, (15th January 2001), p. 10, point 1.1.
[33] However, the programme pays insufficient attention to the fact Article 55 clearly requires that any declarations of not being bound by Article 54 must be made when "ratifying, accepting or approving" the Convention. States that became bound by the Schengen *acquis* after the Amsterdam Treaty, upon membership of the European Union, cannot—on a literal interpretation—subsequently make such declarations.
[34] Colangelo (2009), 814-5.

institutions and bodies of the EU,[35] as well as Member States when implementing EU law.[36] Article 50 of the FR Charter provides that:

> [n]o one shall be liable to be tried or punished again in criminal proceedings for an offence for which he or she has already been finally acquitted or convicted within the Union in accordance with the law.

Van Bockel robustly criticises the opaque wording of this provision.[37] A literal interpretation, for example, does not immediately make clear if the protection applies between countries. These concerns have been warranted, with the opaque wording of the provisions having already spawned litigation before the CJEU.[38] Although there will undoubtedly be further interpretation required, the following appears to be the scope of the provision, as currently understood. First, the guarantee in Article 50 operates at two levels: within the jurisdiction of every Member State, and between Member States. This is stated in the Explanatory Memorandum of the FR Charter,[39] and has been confirmed by the CJEU.[40] Second, as the Court of First Instance made clear, the Article "is clearly intended to apply only within the territory of the Union and the scope of the right laid down in the provision is expressly limited to cases where the first acquittal or conviction is handed down within the Union."[41] Third, as mentioned above, the provisions of the Charter are addressed to Member States "only when they are implementing Union law."[42] The CJEU has a long and contentious history in delineating the circumstances when it will subject Member States' acts to review under its general principles of fundamental rights under Community law (of which *ne bis in idem* is also a part).[43] The FR Charter was intended to limit such interpretative possibilities,[44] but the *Fransson* case has made clear that the CJEU will take a wide interpretation of 'implementing Union law' so as to ensure its powers of review in cases of *ne*

[35] Article 6(1) TEU.
[36] Article 51(1) FR Charter.
[37] Bockel (2010), 18.
[38] Case C-617/10 *Fransson* (26 February 2013).
[39] Explanations Relating to the Charter of Fundamental Rights (OJ C303/02, 14 December 2007), p. 17.
[40] Case C-129/14 *Spasic* (27 May 2014), [6].
[41] Case T-223/00 *Kyowa Hakko* (Judgment of the Court of First Instance of 9 July 2003), [104].
[42] Article 51(1) FR Charter.
[43] For discussion, see Weiler and Lockhart (1995).
[44] See Knook (2005), 371-4.

bis in idem.[45] Nevertheless, even if the Court had adopted a more cautious approach, its jurisdiction will still be considerable in the field of criminal law, given the EU's increasing role in harmonisation in this area.[46] As Knook has argued, the extensive use of EU powers "will coinstantaneously widen the Court's scope of fundamental rights review of Member State measures."[47] This may result in considerable ambiguity given the overlap in *ne bis in idem* provisions. From an intra-State perspective, both Article 50 of the FR Charter, as well as A4P7 of the ECHR,[48] will apply to Member States. And in terms of inter-State obligations, both Article 54 of the CISA and Article 50 of the FR Charter would apply, when the case concerns the 'implementation' of EU law.[49]

8.2.3. The Significance of Protection in the EU

The content of both Article 50 of the FR Charter, and Article 54 of the CISA, will be dissected in more detail below, but for present purposes it is important to emphasise that both provisions place a significant restriction on a large number of European States[50] and their ability to re-prosecute individuals even where crimes have been committed in their territories. They demonstrate that within the EU, where there is a movement towards the harmonisation of criminal laws and significant efforts to improve international cooperation in criminal enforcement, the *ne bis in idem* principle, applying between States, has been seen to be a crucial component. This stands in contrast with the suppression conventions, which are focused more on empowering enforcement than protecting human rights.

---

[45] *Fransson, supra* note 38, [31]. Compare Opinion of Advocate General Cruz Villalón, Case C-617/10 *Fransson* (12 June 2012), [47]-[65].
[46] See generally, Klip (2012).
[47] Knook (2005), 387.
[48] All EU Member States have ratified the Protocol, with the exception of the UK, Germany and the Netherlands. The UK has not even signed the Protocol, although the previous Labour Government had indicated its intention of ratifying it. See Joint Committee on Human Rights, 17th Report (2004-5), para. 28.
[49] It is worth re-iterating that Article 54 CISA does not have such a limitation. On the compatibility of Article 54 with Article 50 FR Charter see Case C-129/14 *Spasic* (27 May 2014). Further difficulties may arise given the difference in wording between the two provisions, although this may be mitigated by Article 53 FR Charter which prevents the Charter from being interpreted in a way which would compromise the human rights protections recognised, *inter alia,* in Union law.
[50] Article 54 CISA even applies to four non-EU countries, namely, Iceland, Norway, Lichtenstein and Switzerland.

However, it is often argued that this inter-jurisdictional application of *ne bis in idem* is exceptional and not representative of any rule of international customary law or reflective of any *erga omnes* obligations.[51] Its role within the EU is said to be borne solely out of the peculiarities of the EU legal order; even the CJEU, when speaking of the rationale for Article 54 of the CISA, has normally emphasised the need to avoid prosecuting an individual for the same acts in multiple Member States on account of an exercise of their right to free movement.[52] Another argument comes from Bernard, who challenges the protective purpose for the *ne bis in idem* principle from a different angle. She claims that the "rationale for its application is more accurately based upon structuring the European or international criminal inter-jurisdictional systems."[53] She does not deny any protective role, but argues that its "first function is linked to the jurisdictional articulation between such concurrently competent courts."[54] In other words, it plays a structural, organising role that supersedes its traditional function. Within the context of the statutes for the International Criminal Court, and the International Tribunals for Yugoslavia and Rwanda, her analysis may be persuasive. However, her argument that the operation of the *ne bis in idem* principle has the same organising role within the EU is under-developed and unconvincing. She claims that the *ne bis in idem* provision in CISA was "related more to legal cooperation between states than to an individual right",[55] but fails to articulate the reasons for this, or even how she purports to ascertain the intentions of the drafters. In fact, her argument is even contradicted by the aforementioned emphasis in the decisions of the CJEU on the rationale being linked to rights of free movement. This is not to deny the principle can also serve to prevent conflicts of jurisdiction, which is an acknowledged[56] and natural consequence of its operation. But there is nothing to suggest that this was even in mind when drafting either Article 50

[51] See discussion of Colangelo below, section 8.3.
[52] See e.g. Joined Cases C-187/01 and C-385/01 *Gözütok and Brügge* [2003] ECR I-1345, [38]; Case C-469/03 *Miraglia* [2005] ECR I-2009, [32]; Case C-436/04 *Van Esbroeck* [2006] ECR I-2333, [34]; Opinion of Advocate General Kokott Case C-17/10 *Toshiba Corporation* [2012] ECR I-0000, (8 September 2011), [100].
[53] Bernard (2011), 4.
[54] Ibid, 2.
[55] Ibid, 4.
[56] Opinion of Advocate General Kokott, Case C-17/10 *Toshiba Corporation* (8 September 2011), [106].

of the FR Charter or Article 54 of CISA. And even if this were a primary intention, the *ne bis in idem* principle would undoubtedly be an ill-equipped tool to "articulate the relationships between concurrently competent jurisdictions."[57] As the Commission has stated in its Green Paper on Conflicts of Jurisdiction:

> …without a system for allocating cases to an appropriate jurisdiction while proceedings are ongoing, ne bis in idem can lead to accidental or even arbitrary results: by giving preference to whichever jurisdiction can first take a final decision, its effects amount to a "first come first served" principle. The choice of jurisdiction is currently left to chance, and this seems to be the reason why the principle of ne bis in idem is still subject to several exceptions.[58]

Intuitively, there is a strong normative appeal to extending the principle beyond EU and Schengen countries. One only needs to consider the possibility of an individual being successively prosecuted and punished in numerous countries to which he travels, for minor offences committed in each country by the same act—a live possibility with many cybercrimes and the current breadth of jurisdiction envisaged in international law—to recognise the need for some fettering of State powers in this regard. Nevertheless, the precise rationale for any internationalised *ne bis in idem* protection is yet to be convincingly distilled. Van Bockel lists no less than twelve principles which are found in national law and which purport to explain its function,[59] acknowledging that this may ironically undermine international application.[60] Furthermore, some rationales that serve well at the national level may not be so easily transposed to the international plane. Stessens and Van den Wyngaert, however, have argued its protective role is equally sensible in both the EU and international spheres, also seeing benefit in the fact that it would facilitate finality of judgments between States.[61] Conway argues in a similar vein, but also spells out the practical implications of the protective role: it avoids the continuous stress and fear of further prosecution, and limits the possibility of conviction of

[57] Bernard (2011), 4.
[58] Green Paper on Conflicts of Jurisdiction, *supra* note 27, 3.
[59] These are, "individual freedom, protection of human rights, protection of the individual from state abuses, justice, proportionality, rule of law, legal certainty, 'juridicial security' (legal certainty), due process, respect for *res iudicata,* procedural efficiency, and the interest of social peace and order." See Bockel (2010), 25.
[60] Bockel (2010), 28.
[61] Stessens and Wyngaert (1999), 780-2.

the innocent, a risk which is heightened with increased prosecutions.[62] This is why the CJEU's emphasis on Union objectives has been criticised,[63] and only the late Advocate General Colomer in *Gözütok and Brügge* has argued for a more universalist understanding of the principle. He contends that it rests on the pillars of legal certainty and equity:[64] a defendant who is either acquitted or convicted of a crime "must have the certainty that he will not be prosecuted again in further proceedings."[65] The principle of equity also serves to prevent penalties from being imposed on the same individual, for the same acts, by requiring that they remain proportionate to their dual purpose of punishing and serving as a deterrent.[66] In fact, AG Colomer even went on to state that it would be "contrary to the very concept of justice to deny the effectiveness of foreign criminal judgments. That approach would both undermine the fight against criminality and the rights of the convicted person."[67] All of the above notwithstanding, academic debate continues regarding inter-State *ne bis in idem* protection, and one of the most prominent expositions of why it should not apply between States, is the work of Anthony Colangelo.

8.3 Colangelo and Dual Sovereignty

Colangelo purports to explain the lack of inter-State *ne bis in idem* in international law by providing a "jurisdictional theory of double jeopardy",[68] which draws heavily on the US dual sovereignty doctrine, developed by the Supreme Court for the federal system. This holds that "[w]hen a defendant in a single act violates the (peace and dignity) of two sovereigns by breaking the laws of each, he has committed two distinct 'offences.'"[69] As we have seen, within the EU, the fact that a single act constitutes separate offences is not a

[62] Conway (2003), 222-4.
[63] It has been argued by Rafaraci and Belfiore (2007), 26 that the CJEU has failed to recognise "the significance of the *ne bis in idem* principle *per se,* i.e. as the expression of a fundamental right" through its emphasis on the objective of facilitating free movement. Bockel (2010), 132, on the other hand, has argued that the Court has emphasised the human rights nature of the provision. The CJEU's purposive interpretation has also been criticised for being ahistorical, since the intentions of the drafters of Article 54 CISA pre-dated the integration of the *acquis* into the EU framework. See Mitsilegas (2009), 145.
[64] Opinion of Advocate General Colomer, *Gözütok and Brügge*, *supra* note 11, [49].
[65] Ibid.
[66] Ibid, [50].
[67] Ibid, [59].
[68] Ibid.
[69] *Heath v Alabama* [1985] 474 US 82, 88.

barrier to an inter-State *ne bis in idem* protection. However, the dual sovereignty doctrine clearly prioritises sovereign powers of punishment over the right of individuals to be free from multiple prosecutions arising from the same acts, and in the US context, his underlying arguments have essentially been confirmed in case-law, which upheld the conviction of an individual who had already been convicted and sentenced for the same acts abroad.[70] Colangelo forcefully argues that this dual sovereignty doctrine[71] is also the basis for the current international law paradigm on *ne bis in idem*. He proposes three rules of international double jeopardy, the most important, for present purposes, being that a "national prosecution applying and enforcing a national law does *not* erect a bar to successive prosecutions by other states with national jurisdiction over the crime in question."[72] With this "jurisdictional theory" of sovereignty, however, he attempts to carve a middle ground between the black and white operation of either a dual sovereignty doctrine, or a *ne bis in idem* provision applying between countries; second prosecutions must also be reasonable, with the factors determining reasonableness drawn directly from the US Restatement on Foreign Relations Law.[73]

One of the most surprising aspects of Colangelo's article is that in his eighty-eight pages of analysis, the CISA is mentioned in only two sentences. The first displayed some misunderstanding of the status of CISA within the EU.[74] The second justified his ignoring of its importance. He stated in the latter "the Schengen Convention is an instrument of cooperation intended to carve out an exception to the general rule [of there being no international prohibition on double jeopardy]."[75] This lack of consideration was regrettable because, as is often the case with hotly contested topics, it can be difficult to establish where the rule ends and the exceptions begin.

---

[70] See *US v Jeong* [2010] 624 F.3d 706. For discussion see Hodgson (2012).
[71] Colangelo (2009), 781, understands sovereignty, in this context, to be equivalent to an entity having independent prescriptive jurisdiction.
[72] Ibid, 797. Original emphasis.
[73] Ibid, 845.
[74] He stated "the European Union put into effect the 1990 Schengen Convention in anticipation of lifting the internal border controls in 1993." Ibid, 814. CISA was actually negotiated outside EU/EC structures.
[75] Ibid.

There are many other problems with Colangelo's suggested approach, primarily relating to some unappreciated distinctions between the international and federal systems,[76] and his faith in 'reasonableness' providing the silver bullet. This latter point raises particular concerns, because, as my second chapter established, it is not even accepted that jurisdictional reasonableness is required under international law. Colangelo is, therefore, trying to remedy uncertainty in international law relating to *ne bis in idem* by utilising an international law rule of equally questionable status. The criteria that he deems relevant to the assessment, and the examples provided, also suggest that his jurisdictional theory will do little to protect against many re-prosecutions. For example, because Colangelo unquestioningly accepts all jurisdictional bases, he would not see any problem with an individual being initially prosecuted on nationality grounds, and subsequently on the basis of territoriality.[77] No attention is given to factors such as the potential unfairness if—pursuant to the first prosecution—the individual had spent the majority of his life in prison. The claim that his jurisdictional reasonableness theory of double jeopardy "explicitly considers individual rights"[78] is open to serious doubt, and the need for further development of the principle at the international level remains. However, this is an area that is ripe with complications in practice.

8.3.1. Recognising the Difficulties

Any attempt to transpose *ne bis in idem* to the international sphere will undoubtedly face staunch opposition. The CJEU has acknowledged that the operation of the principle requires mutual trust in criminal justice systems, recognition of foreign criminal law decisions even when the outcome would differ domestically,[79] and a sharing of values.[80] This trust has been presumed by the CJEU, but as Mitsilegas has noted, "[w]hether such [a] level of trust

[76] For example, the dual sovereignty doctrine was based on the fact that "[e]very citizen of the United States is also a citizen of a State… He may be said to owe allegiance to two sovereigns. And [sic] may be liable to punishment for an infraction of the laws of either." Colangelo (2009), 840 (quoting *Moore v Illinois* [1852] 55 US 14 How. 13, 20.) Such allegiance is not present when an individual is a national of one country, but has committed a crime in various other countries by the same act.
[77] Colangelo (2009), 846.
[78] Ibid, 843.
[79] *Gözütok and Brügge, supra* note 52, [33] and *Van Esbroeck, supra* note 52, [30].
[80] Opinion of Advocate General Colomer, *Gözütok and Brügge, supra* note 11, [55].

actually exists [even within the EU] is an open question."[81] Judging from what States have already consented to in the terms of their respective enforcement powers in suppression conventions,[82] there seems to at least be a platform for garnering a similar level of fragile trust outside of EU frameworks as well. However, even leaving aside Colangelo's jurisdictional and sovereignty arguments, the possibility of *ne bis in idem* being recognised inter-State more broadly in international law, whether in a suppression convention, customary international law, or as an *erga omnes* obligation,[83] will be hampered by the lack of consensus on its core components. While States may agree in principle that an individual should not be re-prosecuted repeatedly for the same offence, the lack of procedural harmonisation across criminal justice systems will cause problems when translating that general agreement into any form of binding commitment. Elementary issues such as the meaning of criminal proceedings,[84] and the types of judgments or decisions that could apply and the meaning of 'finality',[85] will mean delineation of any possible 'core' understanding of the principle, a daunting endeavour. But even if these issues prove to be surmountable, the *idem* challenge remains, and with the advent of cybercrime, this is likely to be one of the most perplexing issues in practice.

8.4 The *Idem* Challenge

There is little consistency in the international instruments dealing with *ne bis in idem* on the concept of *idem*, which could refer to the same *facts* or *acts*, or

---

[81] Mitsilegas (2009), 148.
[82] See chapter four.
[83] Conway (2003), 221 conflates *erga omnes* obligations, and those stemming from *inter partes* agreements, when he states that Article 54 CISA constitutes an *erga omnes* obligation. An *erga omnes* obligation, as the International Court of Justice has recognised, is one that is, by its very nature, of concern to all States: "[i]n view of the importance of the rights involved, all States can be held to have a legal interest in their protection" See Barcelona Traction, ICJ Reports [1970] 3, [33]. See also Picone (2011).
[84] The ECtHRs has provided guidance on this in case of *Engel v The Netherlands* [1976] 1 EHRR 647, which has been adopted by the CJEU in two cases concerning Article 54 CISA: *Fransson*, *supra* note 45, [35] and Case C-489/10 *Bonda* [2012] ECR I-0000 [37].
[85] The CJEU has found that a prosecutorial settlement with the accused will suffice for the purposes of Article 54 CISA (*Gözütok and Brügge*, *supra* note 52), as would a decision holding that a prosecution was time barred even though it did not involve an assessment on the merits of the case (Case C-467/04 *Gasparini* [2006] ECR I-9199). See further on finality Case C-469/03 *Miraglia* [2005] ECR I-2009, and Case C-491/07 *Turansky* [2008] I-11039. There is again some convergence between the CJEU and the ECtHR on the issue of finality: Case C-398/12 *M* (5 June 2014), [38]-[39].

only prosecutions for the same *offence*.[86] The majority refer to 'offence',[87] but Article 8(4) of the American Convention on Human Rights refers to 'same cause', while Article 54 of the CISA applies to 'same acts.'[88] The initial English translation of Article 54, however, referred to same 'offence',[89] which suggests some uncertainty on the initial intentions of the drafters. The applicability of one over the other has a profound impact on the scope of protection. For example, if an individual modifies computer data without authorisation, and is prosecuted for an unauthorised *access* offence, which fails, he could not be re-prosecuted for an unauthorised *modification* offence, if *idem* means 'same acts.' He could if *idem* means 'same offence.'

8.4.1. The CJEU's Approach to Idem

Despite the uncertainties in initial translations of Article 54 of the CISA, the CJEU has now developed a consistent jurisprudence on the question of *idem*, beginning with the *van Esbroeck* decision.[90] Van Esbroeck was first convicted of illegally importing drugs in Norway. He served part of his sentence there, and after being escorted back to Belgium, was then prosecuted and sentenced for *exporting* the same drugs from Belgium to Norway.[91] The Belgian courts sought guidance from the European Court of Justice as to how to interpret Article 54 of the CISA, and its response has been repeated many times since:

> …the relevant criterion for the purposes of the application of that article of the CISA is identity of the material acts, understood as the existence of a set of facts which are inextricably linked together, irrespective of the legal classification given to them or the legal interest protected.[92]

The CJEU found that, in principle, importing and exporting the same drugs, into two different countries, which are classified differently from a legal

---

[86] Conway (2003), 227, refers to these approaches respectively as '*in concreto'* and *'in abstracto*' applications.
[87] See A4P7 ECHR, Article 14(7) ICCPR, and Article 50 of the Charter.
[88] The Harvard Draft Convention on Jurisdiction (1935), also referred to 'same acts' in Article 13, while the 1987 Convention on Double Jeopardy, which as mentioned *supra* note 19 never entered into force, referred to the "same facts."
[89] Bunyan (1997), 120.
[90] *Van Esbroeck, supra* note 52.
[91] Such a case is complicated by the fact that Article 36(2)(a) of the Single Convention on Narcotic Drugs 1961, which was ratified by both countries, states that the importing and exporting of narcotics, 'if committed in different countries, shall be considered as a distinct offence.'
[92] *Van Esbroeck, supra* note 52, [42].

perspective in each country (e.g. export and import) are the 'same acts' for the purposes of *ne bis in idem* protection, if they "constitute a set of facts which are inextricably linked together in time, in space and by their subject-matter."[93] In rejecting an interpretation that would look to the legal classification of the offence, the CJEU's reasoning was clearly based on providing a broader protection for defendants.[94] It emphasised that without "harmonisation of national criminal laws, a criterion based on the legal classification of the acts or on the protected legal interest might create as many barriers to freedom of movement within the Schengen territory as there are penal systems in the Contracting States."[95]

The CJEU has attempted to build a coherent body of case-law on this point, and has repeated on numerous occasions the need for "identity of material acts" from *van Esbroeck*. In *van Stratten*[96] it opined that possession of different quantities of drugs in different countries, and with different accomplices, could still be acts which are "inextricably linked"[97] together, thus barring any second prosecution. Similarly, in *Kretzinger,*[98] it repeated verbatim many of the operative paragraphs from *van Esbroeck* in the context of prosecutions for the transportation of contraband cigarettes between Italy and Germany, which involved successive crossings of the internal Schengen border areas.[99] These were acts that could also constitute a set of facts covered by the 'same acts' criterion, despite the German authorities seemingly trying to circumvent the Article 54 restrictions by prosecuting him for the extraterritorial act of initial import in Greece, rather than the smuggling between Italy and Germany.[100]

These import/export cases have been relatively straightforward for the CJEU,

---

[93] Ibid, [38]. The definitive assessment of this question is, however, left for the national court to decide.
[94] A protective approach was endorsed in the Inter-American Court of Human Rights in the case of *Loayza-Tamato v Peru* [1997] IACHR 6, [66], quoted in Neagu (2012), 967, footnote 58.
[95] Ibid, [35]. Repeated in Case C-150/05, *van Stratten* [2006] ECR I-9327, [47].
[96] *van Stratten supra* note 94.
[97] Ibid, [49]-[50]. From the questions asked of the Court, it does appear that the drugs were from the same consignment, and the offences in both countries from in or around the same period. Ibid. [30].
[98] Case C-288/05, *Kretzinger* [2007] ECR I-6441.
[99] Ibid, [36].
[100] See in particular the formulation of the first question, *Kretzinger*, ibid, [36]. For discussion, see Mitsilegas (2009), 150.

but the coherence of its jurisprudence will be more difficult to sustain as it is faced with more complex criminal transactions. An illustration of such nascent difficulties is *Kraaijenbrink,*[101] which concerned convictions for laundering the proceeds of drug trafficking in Belgium, having previously been convicted in the Netherlands for receiving and handling the proceeds of drug trafficking.[102] Kraaijenbrink claimed that the money laundering operations in both countries concerned the same sums of money, from the same drug trafficking operation,[103] but it was not clear from the documents submitted if that was the case.[104] The referring court from Belgium sought guidance as to how the 'same acts' criteria should be interpreted in a situation where there existed a "common intention"[105] to launder the proceeds of drug trafficking.

The CJEU again re-iterated its requirement for the material acts to be "linked in time, in space and by their subject-matter, make up an inseparable whole",[106] and held that a common criminal intention would not be sufficient to render such acts the 'same', for the purposes of Article 54.[107] On the particular facts of the case, it said where it cannot be clearly established that the money laundered in both countries was the same, such a situation could only constitute the 'same acts' under Article 54 "if an objective link can be established between the sums of money in the two sets of proceedings."[108]

It is not entirely clear what the Court means by this "objective link" addition,[109]

---

[101] Case C-367/05 *Kraaijenbrink* [2007] ECR I-6619
[102] Ibid, [13]-[14].
[103] Opinion of Advocate General Sharpston, Case C367/05 *Kraaijenbrink* (5 December 2006), [30].
[104] Ibid, [23].
[105] *Kraaijenbrink, supra* note 101, [19], [20], [25].
[106] Ibid, [28].
[107] Ibid, [29]. This was consistent with the decision of the Advocate General, *supra* note 103, [44].
[108] Ibid, [31].
[109] It seemingly came from the Commission's submissions in the case which, in attempting to deal with the 'common intention' link between the money laundering acts, distinguished between subjective and objective links. Ibid, [30]. Given that it was distinguishing between a subjective approach which emphasised the intention of the accused, it might be thought that this 'objective link' test is akin to that found more generally in the criminal law, where it denotes a 'reasonable bystander' test. In all likelihood, this was not what was meant. The CJEU here appears to be using the adjective 'objective' in its dictionary sense of the word: it being a question of objective fact not dependent on individual thought for existence. This criterion has previously been used by the CJEU in the competition field, relating to disclosure of documents and the need to establish an objective link between the documents sought and the allegations in the statements of objections. Case C-204/00 *Aalborg Portland* (7 January 2004),

or whether it has altered the prior test from *van Esbroeck*, and it is unlikely to have provided any extra guidance to the national court which had to assess whether different aspects of the money laundering operation (handling v. exchange) in different countries, could constitute the 'same acts.' [110] Nevertheless, there has been some convergence on this issue between European courts: the ECtHR recently adopted the CJEU's 'same act' criteria,[111] in the context of A4P7 of the ECHR, and I argue below that on current academic interpretations of this development, there is a danger of *ne bis in idem* protection between EU Member States, or in any subsequent international agreement, being rendered nugatory in the cybercrime context.

8.4.2. The Dangers of Convergence Between the ECtHRs and the CJEU

A4P7 of the ECHR only applies intra-State. Its wording appears *prima facie* straightforward and unlikely to cause interpretative difficulties for the ECtHRs. The provision has, however, resulted in one of the most incoherent strands of case-law to ever come from Strasbourg. Sub-section 1 of the Article provides that:

> [n]o one shall be liable to be tried or punished again in criminal proceedings under the jurisdiction of the same State for an offence for which he has already been finally acquitted or convicted in accordance with the law and penal procedure of that State.

Adopting a purely literal interpretation of the Article, it appears to prohibit a State from re-prosecuting or re-punishing an individual for an *offence* for which he has already been acquitted or convicted in criminal proceedings.[112] However, as I have analysed elsewhere,[113] the ECtHRs has oscillated between numerous interpretations of the provision, ranging from a consideration of

---

see in particular [108]&[129]. This was not referred to, however, and it is not clear if it assists in interpreting this phrase

[110] The Advocate General had spoken less ambiguously and provided examples of situations where money-laundering activities could constitute the 'same acts', and where they would not. See the AG Opinion in *Kraaijenbrink*, *supra* note 103, [32]-[33].

[111] *Zolotukhin v Russia* (No. 14939/03, 10 February 2009), which was affirmed in *Pirttimäki v Finland* (No. 35232/11, 20 May 2014).

[112] In fact, it goes so far as to provide a right not to be *liable* to be tried twice. This threefold protection has been recognised in *Nikitin v Russia* (No. 50178/99, 20 July 2004).

[113] Article in preparation.

whether the individual is being re-prosecuted for the same *conduct*,[114] a strict legal classificatory approach which looks at whether both cases involved the same *offence* (as a literal interpretation of A4P7 would require),[115] and an 'essential elements' approach, whereby the Court analysed the offences charged in each set of proceedings, and determined whether or not they shared the same *essential elements* relating to the same acts.[116]

Recently, the ECtHRs has acknowledged that these divergences "engendered legal uncertainty incompatible with the fundamental right not to be prosecuted twice for the same offence."[117] A criminal act can usually constitute a range of different criminal offences, and focusing only on the 'offence' for which the person is prosecuted, exposes them to separate prosecutions for each offence. Therefore, the ECtHRs has abandoned the "essential elements" and "legal classification" approaches, the latter being "too restrictive on the rights of the individual."[118] In *Zolotukhin v Russia*,[119] an individual was prosecuted for three separate incidents which occurred on the same day: verbal abuse of two individuals in a police station, and then two separate incidents of abuse against a more senior officer, first in his office, and then in his car. In respect of the latter incidents involving the more senior officer, only criminal proceedings were brought – thus, no issue arose under A4P7.[120] However, in respect of the first incident, Zolotukhin was charged for an administrative offence (on the day of the incident) as well as in criminal proceedings at a later stage. The ECtHRs found a breach of A4P7,[121] by essentially adopting the CJEU's test for *idem* (e.g. facts which are substantially the same, and inextricably linked together in time and space).[122]

This reversion to a form of 'same act/conduct' test has been praised by commentators,[123] despite being a strain from the perspective of literal

[114] *Gradinger v Austria* (No. 15963/90, 23 October 1995).
[115] *Oliveira v Switzerland* (No. 25711/94, 30 July 1998).
[116] *Franz Fischer v Austria* (No. 37950/97, 29 August 2001).
[117] *Pirttimäki*, *supra* note 111, [49], quoting *Zolotukhin*, *supra* note 111, [81]-[84].
[118] *Zolotukhin*, *supra* note 111, [81].
[119] Ibid.
[120] Ibid, [93].
[121] Ibid, [97] & [120]-[122].
[122] Ibid, [92]-[94].
[123] See e.g. Bockel (2010), 200.

interpretation, but the ECtHRs is also said to have contradicted the CJEU in the process of adopting the latter's case-law for A4P7.[124] Neagu draws particular attention to the ECtHRs' *obiter* comment that there was no "temporal or spatial unity between the three episodes [because] it was not a continuous act but rather different manifestations of the same conduct shown on a number of distinct occasions."[125] This does indeed appear *prima facie* inconsistent with the approach of the CJEU, which has found there can be spatial and temporal unity despite the offences occurring in different countries, at different times, and even with different individuals involved in the facilitation of the offence. Neagu, however, purports to reconcile the approaches of the two courts, by drawing on "unwritten principles in national jurisdictions on offences committed against certain social values related to natural persons."[126] This general rule states that when the same conduct is directed "against *different persons* [they are…] to be considered as two different acts, even if committed in the same temporal and spatial circumstances."[127] Neagu contends that this resolves the apparent contradiction between the ECtHRs in *Zolotukhin*, and the case-law of the CJEU. The ECtHRs introduced "new criteria in the back door"[128] and extended the interpretation of the CJEU. Therefore, for Neagu, "the criteria for establishing a breach of the *ne bis in idem* principle as regards the *idem* concept in respect of *certain offences against natural persons* should be read as a set of facts inextricably linked together in time and space, as well as by their object and *subjects*."[129]

It is not entirely clear which 'unwritten principles' Neagu has in mind, but in terms of the common law, he seems to be referring to the rule against duplicity in indictments. This rule, at its most general, requires that each count in an indictment charges only one offence, but in the case of crimes against persons, modern practice has been to have a separate count per victim.[130] I contend that Neagu's explanation of *Zolotukhin* is flawed, and if adopted by the CJEU, as

[124] Neagu (2012), 970-1.
[125] Zolotukhin *supra* note 111, [92].
[126] Neagu (2012), 971.
[127] Ibid. Original emphasis.
[128] Ibid.
[129] Neagu (2012), 971. Original emphasis.
[130] See e.g. *Mansfield* [1977] 1 WLR 1102. Here seven individuals died from a single fire allegedly started by Mansfield, and the indictment contained a count per victim.

he proposes, would lead to a complete undermining of the protection afforded in Article 54 of CISA. For example, it would mean that if an individual perpetrated an act of fraud on numerous individuals in different countries from the same act (e.g. simultaneously sending a phishing email to thousands of individuals in numerous countries), each would have to be considered as separate acts, and therefore each could be prosecuted consecutively.

However, there are a number of reasons why Neagu's analysis must not be dismissed offhand. First, due to the incoherent history of case-law from the ECtHRs, which at times mistakenly integrated domestic charging considerations into its approach to A4P7,[131] these interpretative difficulties may well re-arise in this setting. Second, since the jurisprudence of the CJEU and ECtHRs has begun to converge on many aspects of their interpretations of *ne bis in idem*,[132] there is a distinct danger that mistakes in one judicial arena will be transposed to the other. Finally, the similarities between legal tests such as the rule against duplicity, and the approach to *idem* before the ECtHRs and CJEU, make a seeping of considerations from the former into the latter areas of law, a distinct possibility, particularly in light of Neagu's analysis.

---

[131] In *Franz Fischer v Austria* (No. 37950/97, 29 August 2001), [25] it was said: "[t]he Court, like the Austrian Constitutional Court, notes that there are cases where one act, at first sight, appears to constitute more than one offence, whereas a closer examination shows that only one offence should be prosecuted because it encompasses all the wrongs contained in the others … Thus, where different offences based on one act are prosecuted consecutively, one after the final decision of the other, the Court has to examine whether or not such offences have the same essential elements." Under this test, the Court does not look at what A4P7 seems to require, which is simply whether an individual has been tried again in separate proceedings for the same offence, or look at whether an individual is being prosecuted for the "same conduct"; now it would dissect the offences charged in each set of proceedings, in order to assess if only one offence should have been prosecuted. This was still, however, actually quite a narrow approach to A4P7. In theory, it was only if offences charged in separate criminal proceedings shared 'essential elements' that A4P7 would intervene. This means an individual responsible for killing with a knife could, for example, be prosecuted for murder, and subsequently for wounding if the former failed, as these offences do not share essential elements. But application of this test by the ECtHRs was incoherent and inconsistent. In the decision in *Franz Fischer* itself it found a violation of A4P7 and that there was no difference in the essential elements of crimes which entailed: 1. Causing death by negligence, with the additional aggravating factor of drunk driving, and 2. Drunk driving. It did so by focusing on the elements of the administrative drunk driving offence, and whether the elements of this also existed in the former offence. The first offence was not, however, 'drunk driving with the additional element of causing death by negligence', rendering this test a muddle and subsequent applications suffered from similar confusion and unpredictability.

[132] Beyond the convergence on *idem*, see *supra* note 84 on the meaning of criminal proceedings, and *supra* note 85 on the meaning of finality. This convergence is encouraged by provisions such as Article 6(3) TEU and Article 52(3) of the Charter.

8.4.3. Rule Against Duplicity v Ne Bis in Idem

If one compares the substance of the rule against duplicity enquiry with that which has been interpreted as being necessitated by Article 54 of CISA, the similarities are striking. Each can be seen to evince a general rule, to which an exception is then carved out. Inherent in Article 54 of CISA is that each country is free to prosecute acts deemed to be criminal offences in their territories, unless another country has tried and finally disposed of a criminal case against that individual for those same acts. Meanwhile, the rule against duplicity states the general rule that not more than one offence can be charged in each count, but there is also an exception to this, which is almost the 'same acts' test from the CJEU verbatim. In *DPP v Merriman*, Lord Diplock, for example, stated that:

> [w]here a number of acts of a similar nature committed by one or more defendants were connected with one another, in the time and place of their commission or by their common purpose, in such a way that they could fairly be regarded as forming part of the same transactions or criminal enterprise, it was the practice, as early as the 18th century to charge them in a single count of an indictment.[133]

The approaches of the CJEU and ECtHRs (in the context of Article 54 of CISA, and A4P7 ECHR respectively) equally consider whether there is spatial and temporal unity and acts which by their subject matter make up an "inseparable whole."[134] The purpose of the exception, like the internationalised *ne bis in idem* principle, is also partly explained by the potential injustice and unfairness that can eventuate from the legal characterisation of the same act as constituting numerous offences.[135] Moreover, the reason why breach of the rule

---

[133] *DPP v Merriman* [1973] AC 584, 607. Rule 14.2(2) of the Criminal Procedure Rules is said to have been derived from this judgment. See Hooper and Ormerod (2010), para. D11.44. The rule states: "More than one incident of the commission of the offence may be included in a count if those incidents taken together amount to a course of conduct having regard to the time, place or purpose of commission." Similarly, in the High Court of Australia in *Walsh v Tattersall* [1996] HCA 26; [1996] 188 CLR 77, 107 Kirby J stated "Exceptions to the general rule against duplicity have been allowed where the multiple acts relied on by the prosecution are so close in time and place that they can be viewed as one composite activity; where the offence is one that can be classified as continuing in nature; and in other anomalous cases."

[134] *Kraaijenbrink supra* note 101, [28]. The same judgment makes clear that although 'common purpose/intent' (also mentioned in *Merriman*) cannot be determinative in the 'same acts' test in and of itself, it is implicit in the judgment that this could be a relevant consideration for the national court. Ibid, [29]&[36].

[135] In *R v Harris* [1969] 1 WLR 745, 746, which concerned a conviction for a count of buggery and a count of indecent assault arising from the same incident, Edmund Davies LJ said "It does

against duplicity results in the quashing of convictions has been explained to be intimately related to the English equivalent of *ne bis in idem* (the plea of *autre fois convict*). In *Wells*, Will J. explained that:

> a conviction ought to specify the particular offence of which the man was convicted, otherwise … if a man were charged again with one of the two alternative offences mentioned in his conviction it would be impossible to say that the plea of autre fois convict would be satisfied by producing the document which contained the offence of which he had been previously convicted.[136]

These similarities and connections are apt to mislead without a clear articulation of the significant differences between the rule against duplicity and the *ne bis in idem* principle as found in Article 54 of CISA. Most obviously, the former is an internal procedural rule which asks whether there is more than one crime per count, while the 'same acts' test of the CJEU is an inter-State obligation concerned with whether a country is prosecuting someone for the same acts that have already been dealt with by another country. Another notable difference is that even if a national court does find that an individual has been prosecuted for the same act previously, it does not deny that separate offences actually occurred—it simply bars the second State from re-prosecuting those acts.[137] On the other hand, if a number of acts are characterised in an indictment as constituting only one offence, and the courts uphold this prosecutorial decision, then only one offence can be said to have been committed.

Their *raison d'être* also obviously diverge. However, like the *ne bis in idem* rationale, the case-law around the duplicity rule is inconsistent in explaining its purpose. In *R v Marchese*, for example, two practical reasons for the rule were provided: avoiding the danger in jury trials of different members deciding counts on the basis of separate considerations, and ensuring that judges know the basis upon which juries convicted for sentencing purposes.[138] Some

---

not seem to this court right or desirable that one and the same incident should be made the subject-matter of distinct charges, so that hereafter it may appear to those not familiar with the circumstances that two entirely separate offences were committed. Were this permitted generally, a single offence could frequently give rise to a multiplicity of charges and great unfairness could ensue."

[136] *R v Wells, Ex parte Clifford* [1904] 91 LT 98, 99.

[137] This, it will be re-called, is in direct contrast with the approach of the US under the dual sovereignty doctrine. See *supra* section 8.3, and Colangelo (2009), 779.

[138] *R v Marchese* [2009] 1 WLR 992, [44].

Australian courts have explained its function in broader terms, emphasising considerations of fairness (e.g. ensuring the defendant knows the full case against him),[139] but have also mentioned many of the practical points related to the administration of justice.[140] Therefore, although both *ne bis in idem* and the duplicity rule are concerned with fulfilling protective functions for the defendant, they also serve distinct purposes. Another radical difference is the potential implications for prosecuting authorities in the application of the respective rules. The effect of Article 54 of CISA can be to bar another State from prosecuting an individual. On the other hand, motions to quash indictments for duplicity can usually be met by amending the indictment,[141] and even if quashed, further proceedings can be brought in the form of a fresh committal. Finally, the judicial enquiry in each is very different: when considering duplicity, the judge looks at the wording of the count;[142] when Article 54 of CISA is considered by national courts, they consider previous judicial processes in another country.

These stark differences highlight the analytical weakness of Neagu's attempted entwining of these areas. His suggestion that the ECtHRs' reasoning in *Zolotukhin* involved an extension of the CJEU's approach to Article 54 of the CISA would eviscerate the protection afforded to the individual by the latter, if ever adopted in practice.

This confusion arose from the ECtHRs commenting on the fact that there was no temporal and spatial unity between the three incidents at issue in *Zolotukhin* and that they did not involve "a continuous act but rather different manifestations of the same conduct shown on a number of distinct occasions."[143] This *dicta* is confusing because the ECtHRs broke down the

[139] See e.g. *Johnson v Miller* [1937] HCA 77; [1937] 59 CLR 467, 497-8.
[140] See e.g. *S v The Queen* [1989] HCA 66; [1989] 168 CLR 266, 284-5. A synthesis of these various reasons can be found in the judgment of Kirby J in *Walsh v Tattersall* [1996] HCA 26; [1996] 188 CLR 77.
[141] Indictments Act 1915, s. 5(1). See also *R v Marchese* [2009] 1 WLR 992, [47]. Some courts seem content to resist a motion for quashing provided there has been no unfairness, in that the defendant understood all of the allegations against him. Others have stressed that due to the broader purposes of the rule against duplicity, it is not sufficient only to show that the defendant has not been prejudiced. See e.g. *Rixon v Thompson* [2009] VSCA 84, [88].
[142] See Hooper and Ormerod (2010), paras. D11.41-54.
[143] *Zolotukhin supra* note 111, [92].

events in *Zolotukhin* as the Russian Government did in its charges, with language that was nearly identical to its approach to *idem* under A4P7. But paragraph 92 of the ECtHRs decision should not be read as an incorporation into its approach to A4P7 of any domestic charging rule relating to a succession of similar acts being treated as different offences if committed against different individuals. There is not even consistency to this effect in domestic charging decisions,[144] and even if there was, the ECtHRs has no role in the characterisation of acts as separate offences. If the Russian Government had decided to characterise all of the acts as one crime in its charges (e.g. disorderly conduct), the ECtHR could only intervene if there were two separate criminal proceedings for the same facts.

8.4.4. Idem in the Cybercrime Context

Idem, the rule against duplicity, and equivalents in other jurisdictions, beg the question 'what is an offence?', but do not provide any clear-cut answers. As one Australian judge has commented, "the courts have never managed to produce a technical verbal formula of precise application which constitutes an easy guide … as to whether the common law rule [against duplicity] has been infringed." [145] This difficulty in mapping physical acts onto legislative provisions, and the fact that numerous offences can be constructed out of the same conduct, has resulted in *idem*, in both Article 54 of CISA, and A4P7, being interpreted as meaning the 'same acts.' Like the rule against duplicity, this is a malleable tool that grants significant discretion to those interpreting it in practice;[146] the protection can be over-inclusive or under-inclusive with few analytical tools available to generate consistency. Examples of some run-of-the-mill cybercrimes will suffice to illustrate this:

---

[144] See e.g. *Jemmisson v Priddle* [1972] 1 QB 489.
[145] *Stanton v Abernathy* [1990] 19 NSWLR 656, 666 per Gleeson CJ.
[146] See e.g. in the context of the operation of the mandatory bar contained in Article 3(2) of the European Arrest Warrant Decision (2002/584/JHA, 13 June 2002), the decision in C-261/09 *Mantello* [2011] 2 CMLR 5 (16 November 2010). Article 3(2) prevents surrendering pursuant to the decision, *inter alia*, if the requested person has been finally judged by a Member State for the same acts. The CJEU interpreted the provision in line with its caselaw under Article 54 CISA, and held that the Mantello could be surrendered for participation in a drug trafficking operation and a possession offence, despite having been previously convicted for the importation of drugs during the same period, and the fact that the referring German court would not have allowed the second set of proceedings under its domestic law. See *Mantello*, ibid, [29] & [51].

- An individual is prosecuted in country A for the uploading of child sexual abuse images. This content is consumed months later by citizens of country B. Given the temporal gap between 'acts', he could subsequently be prosecuted in country B for the publication there, without infringing the *ne bis in idem* principle.

- An individual is prosecuted in country C for sending emails pursuant to a phishing scam. Over the course of a number of weeks the individual used different forms of malware, and losses were sustained in different countries. Given the time frames, and the distinct tools involved, the individual could subsequently be prosecuted in country D.

In the realm of cybercrime, there will be many ways to distinguish acts, according to the test proposed by the CJEU, so as not to bar further prosecution. At the same time, the 'same acts' approach to *idem* may result in individuals escaping accountability for the full extent of their criminal conduct. This was a significant concern for my Eurojust interviewee (**EJ**); the aforementioned current paradigm of focusing on the domestic harm resulting from domestic actors[147] precludes appreciation of the wider picture, and the potentially larger pool of actors, and victims, in different jurisdictions. EJ stressed the danger of prosecuting an individual for "a small part" of a much bigger transaction, which thus prevents further prosecution in other jurisdictions.[148] This has also been a concern for academic commentators, who have as a result, advocated the "same offence" approach to *idem*,[149] and for members of the CJEU. Advocate General Sharpston in her *Kraajibrink* opinion stressed the "undesirable results" which would eventuate from too literal an application of *van Stratten*:[150]

> A conviction for possessing or handling a small quantity of drugs in one Member State should not in my view automatically foreclose further criminal proceedings for possessing or handling substantially larger quantities of the same drugs in another, irrespective of whether they form part of the same consignment.[151]

The problem, however, is that the "same acts" test by the CJEU provides no mechanisms for distinguishing such situations.

---

[147] See chapter six, section 6.4.
[148] Eurojust Interview.
[149] Stessens and Wyngaert (1999), 791.
[150] Opinion of Advocate General Sharpston, *Kraaijenbrink*, *supra* note 103, [36].
[151] Ibid.

8.5 Conclusion

As we have seen, *ne bis in idem* is an important inter-State protection within the EU, but any international agreement regarding further inter-State protection is laden with complexity. While there are flaws in Colangelo's 'dual sovereignty' arguments, the lack of procedural harmonisation of criminal justice systems will mean that any attempt to garner consensus on the precise scope of any further protection (for example, on issues such as the meaning of criminal trials, or finality of judgments) will be slow to emerge. It would also necessarily require trust in foreign criminal justice systems, as the CJEU has recognised, and a curtailment of domestic powers of punishment.

Particular difficulties arise from the transnational nature of modern forms of criminality, where acts can have consequences in different countries, within close temporal proximity. Deciding whether these acts or consequences result in *distinct offences* can be controversial and challenging (e.g. whether the accessibility of a website can constitute distinct offences in all countries from which it is accessible), but even if it is clear that separate crimes have been committed, the *ne bis in idem* principle, as applied within the EU, can require consideration of whether these distinct offences constitute *distinct acts*. The jurisprudence of the CJEU demonstrates that there are already difficulties in delineating when acts should be considered the 'same' for the purposes of the *ne bis in idem* principle. It has generated some consistency in the drug trafficking cases, by denying that the import and export of drugs, in different countries, which constitute distinct offences, necessarily results in these acts being seen as 'different.' But the nature of cybercrime is primed to further complicate application of the 'same acts' test, as my simple examples above demonstrated. I have explained why Neagu's attempted reconciliation of the jurisprudence of the CJEU and ECtHR was flawed, and why acts can be considered the 'same', for the purposes of *ne bis in idem,* even if different victims are involved. However, there are undoubtedly further complications that lie in wait for the CJEU on the question of *idem*.

These difficulties no doubt partly explain the PC-CY's decision not to address the *ne bis in idem* principle in the Convention. Nevertheless, like Stessens and

van den Wyngaert,[152] I am convinced that in a globalising world, *ne bis in idem* is an essential guarantee for individuals who could face prosecution across the globe. Cybercrime often entails elements of criminality, and its effects, in numerous territories and due to the greater number of countries potentially interested in prosecution and with jurisdiction to do so, there is a resulting likelihood of numerous exercises of jurisdiction, in relation to the same conduct.

The CJEU's 'same acts' test may well leave considerable discretion to national courts and, in practice, the principle could oscillate from being over-inclusive to under-inclusive, with little to assist in the prediction of any given outcome. But just as the rule against duplicity "has always been applied in a practical, rather than strictly analytical, way for the purpose of determining what constituted one offence",[153] the same practical attitude is likely to guide interpretations of the principle of *ne bis in idem*. The CJEU's 'same acts' test is the most suitable current tool for striking the difficult balance between allowing States to prosecute individuals for different acts, whilst preventing the injustice of repeated prosecutions for the same conduct. In my conclusion, I will address some of the mechanisms that may serve as catalysts for developing further consensus on this principle, and building it into mechanisms for inter-State cybercrime cooperation.

[152] *Supra* note 5.
[153] *DPP v Merriman* [1973] AC 584, at 607C *per* Lord Diplock.

Chapter 9: Conclusion

9.1 Introduction

This thesis has introduced some analytical balance into the claims that States are impotent to prevent cybercrime,[1] by highlighting the role and importance of the cybercrime suppression project. The Cybercrime Convention itself is still in its infancy, but as ratification is steadily rising, and with proposals emerging to further entrench enforcement powers, the time was ripe for a review of what it has done, what its provisions can mean in practice, and what may be in store. This thesis has sought to provide this analysis through a jurisdictional lens. It has argued that the Convention—like other suppression conventions before it—is imbalanced in the transnational jurisdictional problems which it seeks to ameliorate, and that the resulting problems are only going to be exacerbated given its current trajectory.

In chapter three I highlighted two important trends in the suppression process. The first is that the problem of jurisdictional concurrency, a problem that has long been with us, is being ignored or underestimated. Traditionally, State practice, as can be discerned from the drafting of suppression conventions, has been to prioritise the prevention of any 'jurisdictional gaps' over any desire to avoid concurrent jurisdiction over criminality. This continues to be the case, and while one may have assumed that the multijurisdictional nature of cybercrime would have resulted in some pause for thought, the Convention even welcomes seizures of jurisdiction on extraterritorial grounds, despite the breadth of territorial jurisdiction when applied to cybercrime.[2] This movement can also be seen elsewhere (for example within the EU) and is not short of support in the literature, even in relation to cybercrime, despite the lack of existing solutions for dealing with cases of concurrency.[3] The assumption is often that concurrency is not problematic in practice, due to the lack of enforcement and because difficulties dissipate when harmonisation occurs.[4] While it is well known to be a

[1] Brenner (2014).
[2] See chapter five.
[3] See discussion of Ryngaert and Luchtman in chapter two, section 2.6.
[4] See chapter six, section 6.1.

'theoretical' problem, it has been mentioned many times in the literature and during my interviews that it is nothing more than that. The fact that the "paper rules"[5] of most States could apply to most cybercrimes does not mean they will result in jurisdictional exercises and 'turf battles.' Therefore, for many, the challenge is rather to get anyone to assume the helm in a cybercrime prosecution, and flexibility in jurisdictional bases should be maintained so as not to hamper the few investigations that do make their way into courtrooms.

This latter point, I have argued, lends itself to the second trend in the suppression process: the expansion of procedural enforcement powers and the intensification of relationships between TGNs, as well as transnational interactions between LEAs and service providers. As chapter four has demonstrated, the scope of the investigative powers provided in the Convention is already significant. We have seen innovations such as the creation of 24/7 networks and the enablement of expeditious requests for preservation. Service providers within a given jurisdiction can be asked to provide data held extraterritorially as the *Microsoft Warrant* case has shown, which seems to be permitted by Article 18 and/or Article 32(b) of the Convention, despite this seemingly constituting an extraterritorial exercise of enforcement power. Foreign service providers are neither out of reach on some interpretations of Article 32(b), and even the open 'web' itself is a powerful investigative tool (Article 32(a)). But the trajectory of suppression conventions is always towards the further intensification of procedural powers and the current proposals for a new protocol to the Convention are illustrative in this regard. Some of the proposals are striking for the depth of powers envisaged, such as contacting service providers abroad (even where the data is stored in a third country) or being able to hack into foreign computer systems in exigent circumstances. State practice, however, is indicative of support growing for such far-reaching enforcement powers, as recent Dutch LEA actions and US legislative proposals have demonstrated.[6] Moreover, the DRIP Act 2014 is an undisguised attempt to transform what was previously a 'cooperative' relationship with foreign service providers, into a compulsory one, and therefore an attempt to extraterritorially enforce UK procedural powers.

[5] Schultz (2008), 813.
[6] See chapter four, section 4.2.3.2.

What was disguised, or at least not recognised or discussed, were the hitherto sacrosanct limitations in international law on such extensions of enforcement power. But this piece of legislation is simply symptomatic of the mind-set which we see driving the cybercrime suppression project.

I have also argued that concurrent jurisdiction in the context of cybercrime is problematic even where harmonisation of offences occurs. Chapter five demonstrated the breadth of territorial jurisdiction, when applied to cybercrime, and the ways that the objective and subjective principles of territoriality have mapped onto this phenomenon. The previous three chapters then demonstrated why arguments of concurrency being a 'non-problem' are unconvincing in the current environment. In chapter six we saw that conflicts regarding forum in transnational cybercrime cases were not reported between prosecutors and investigators in EC3, Eurojust or SOCA, which was partially explained by the current costs and complexities for many LEAs pursuing these investigations. However, that was not to say that problems were not envisaged, with interview participants noting the rise in the number of cases being dealt with by Eurojust and EC3, and the complexity entailed in their coordination. A number of forces were also identified which can incentivise the unilateral pursuit of cases, such as when domestic police funding is measured by the number of cases sent to domestic prosecuting authorities.

Moreover, while those operating within the networks of prosecutors and investigators may see no signs of conflict between them, one only needs to look at the consequences of the various cybercrime extradition requests in the UK to see how non-conflict between TGNs can translate into significant difficulties between the States concerned. My overview in chapter seven of UK cybercrime extraditions demonstrated the political potency of these cases, particularly when there was concurrent jurisdiction involving British nationals. The range of countries that can claim territorial jurisdiction over a cybercrime was inevitably going to generate difficulties, especially when it was combined with the trend in extradition law towards the removal of barriers to cooperation, a claim in the literature that was fully supported by my analysis of UK extradition law. The introduction of a forum bar in the UK, which was shown to be directly related to cybercrime extradition requests, bucks this trend, and is notable for having

occurred as a result of the transgovernmental interactions of two close law enforcement allies. The difficulties that emerged in this context, between two 'friendly' nations, are a cautionary tale for other States.

Chapter eight demonstrated another problem arising from jurisdictional concurrency over cybercrime: the risk of multiple prosecutions between parties to the Convention and the failure to address the *ne bis in idem* principle. The omission is understandable, as many countries may still disagree with any such curtailment of their prosecutorial powers, adopting Colangelo's 'dual sovereignty' arguments, and there is considerable uncertainty about many aspects of the principle for those countries that are bound by it within the EU. Although I was able to demonstrate how Neagu's attempted reconciliation of the jurisprudence of the CJEU and ECtHR (which would have rendered any *ne bis in idem* protection meaningless in the context of cybercrime) was flawed and caused by a mistaken reliance on domestic charging considerations, the application of the CJEU's current 'same acts' test will undoubtedly prove difficult in the cybercrime context, as my hypothetical examples demonstrated, but the risk of re-prosecutions outside of the EU is an even greater concern.

While many of the problems with jurisdictional concurrency traced in the above chapters have related to the practices of the US, I have also argued that the emergent issues must be placed in the context of the aforementioned trend towards further expanding enforcement jurisdiction and procedural powers in suppression conventions. If States are provided with further tools to assist their unilateral investigations, there is a strong likelihood of jurisdictional concurrency being a broader problem, particularly as States develop their capacities to pursue cybercrime investigations and prosecutions against domestic as well as foreign offenders. These jurisdictional trajectories are currently 'uneasy bedfellows' in suppression conventions.

In the final two sections of this thesis, I will outline some of the most important choices States have to make in ameliorating investigative and enforcement challenges and the problems arising from jurisdictional concurrency. I foresee that addressing these issues will entail further utilisation of the role of TGNs and other networking interactions. Most importantly, I argue that the law must

develop so as to ensure that rights-based concerns are recognised and respected in both areas.

9.2 Addressing Investigative Challenges: Extraterritorial Data and the Role of Networks

While I foresee knock-on consequences with the expansion of investigative powers over cybercrime, I am under no illusion about the necessity for doing so. Cybercrime laws are undoubtedly under-enforced because, *inter alia*, these investigations and prosecutions demand a technical expertise that many States are some years from developing; cybercrime is unlike other transnational crimes (e.g. drug or people trafficking) where general policing methods and knowledge can be transposed from one criminal activity to another. In chapter four I also identified a number of asymmetries, with current conditions favouring policing hegemons such as the US (given the density of Internet architecture and service providers based there), or those with political clout over foreign service providers (such as the UK). These asymmetries themselves can exacerbate difficulties with jurisdictional concurrency, as they can incentivise unilateral pursuit of cases by only a limited 'club' of LEAs, whilst other ill-equipped police forces may be only too happy to externalise the cost of prosecutions. This ultimately places the suppression project under considerable strain, as one of the foundational ideas behind such conventions is that once laws are harmonised, domestic enforcement will assist to suppress the threat.

Any amelioration of this situation will be dependent on numerous and multifaceted factors and most obviously requires all States to invest in their domestic cybercrime policing capacities. But it will also invariably require further agreement on how, and in what circumstances, LEAs can gain access to data outside their territories. The territorial limitations of enforcement jurisdiction could (theoretically) frustrate even basic investigative techniques, such as accessing a suspect's data or communications on an unlocked mobile phone or laptop (although as we have seen, this is not preventing such access, and customary rules of international law may well develop so as to permit access in these circumstances.) This is why we are seeing calls for "evidence 'location'

to be reconceptualized",[7] so as to find mechanisms for facilitating further LEA access to extraterritorial data. It is also one of the reasons why we are currently seeing States reverting to their Westphalian toolkits and attempting to create and strengthen "cyberborders"[8] so as to ensure "data sovereignty."[9] 2014 will likely be seen in the future as a watershed moment in the history of the Internet, with the first laws passed that will compel service providers who operate (e.g. are accessible) within their territory to store data pertaining to their residents/citizens on servers within the jurisdiction.[10] The catalyst behind these laws was undoubtedly data protection concerns, particularly following the Snowden revelations and the widespread access to data of foreign nationals by US and UK intelligence agencies. However, they would serve a dual purpose, as they will also allow domestic LEAs to gain access to this data for their own criminal investigations. This has been previously unavailable to many LEAs due either to the lack of cooperative relationships with (often US based) service providers,[11] or the ineffectiveness of MLA requests, and is frustrating even rudimentary (non-cyber) criminal investigations.

The technical feasibility of such laws for many service providers is not yet known,[12] nor are the long term consequences for the free and open Internet. As Fehlinger notes, "[w]hat is missing is … a global debate on unintended consequences."[13] It is outside the scope of this thesis to speculate further about the future of these 'data sovereignty' laws, but I can make the limited prediction

---

[7] UNODC Cybercrime Study (2013), xi.
[8] Kohl (2014). See also Kohl (2007), 278-287.
[9] Filippi and McCarthy (2012).
[10] Russia, for example, has enacted Federal Law No. 242-FZ 'On Amendments to Certain Laws of the Russian Federation in Order to Clarify the Procedure for Personal Data Processing in Information and Telecommunications Networks.' It requires Internet operators, *inter alia*, to store Russian citizens' personal data only in databases located within Russia, and also to ensure retrieval of this data is only done from within the territory. Failure to do so can result in that service being blocked and a "register of violators of personal data subjects" rights is also to be maintained. For discussion see http://www.lexology.com/library/detail.aspx?g=665dd256-a402-4798-960b-8ebea29d2a22 (Accessed 20/12/2014). There are also numerous calls now for 'clouds for Europe.' See e.g. http://www.zdnet.com/cloud-for-europe-launches-as-sap-backs-eu-rules-on-data-privacy-7000023205/ (Accessed 20/12/2014).
[11] The Google Transparency Report states that only 3% of user data requests from Russia are complied with: http://www.google.co.uk/transparencyreport/ (Accessed 20/12/2014).
[12] A simple illustration will suffice: if an Irish national posted a photo of a Russian citizen on his own Facebook timeline, from Ireland, would this have to be stored on Russian servers in accordance with Federal Law No. 242-FZ? The details of the Russian law will be spelled out in regulations, but they are unlikely to provide answers to even these basic issues.
[13] Fehlinger (2014).

that attempts to hermetically seal national 'cyberborders' are unlikely to succeed fully in their objectives. The analogy by Swire of elephants and mice is particularly apt: while large multinationals such as Facebook (elephants) may be easily targeted by such laws, "[t]he situation is quite different for mice, which are small, nimble, and breed annoyingly quickly … Would-be regulators can run around furiously with a broom, but with little chance of getting rid of all the mice."[14] But if data sovereignty laws do proliferate further, and succeed in impeding foreign LEA access to data,[15] or if Microsoft succeeds in the *Microsoft warrant* case, even the current policing hegemons may be hampered in their transnational cybercrime investigations.

These difficulties and movements point to finding mechanisms for improving access to data from foreign service providers being one of the most pertinent issues that must be addressed by States. Indeed, finding solutions to this end would relieve much of the need for other, more drastic, procedural tools, such as permitting hacking into foreign servers in 'exigent circumstances.' Therefore, one of the issues with which I am in agreement with the Transborder Group is that "in the absence of an agreed upon international framework with safeguards, more and more countries will take unilateral action and extend law enforcement powers to remote transborder searches either formally or informally with unclear safeguards."[16] The question is how, and under what conditions and safeguards, further transnational access to data from foreign service providers should be permitted.

Outside of LEA communities, the rallying cry is for MLA to be improved. It has been recognised in the US that "non-US governments seeking [data from US based service providers] can face a frustrating delay in conducting legitimate

[14] Swire (1998), 1019.
[15] The Russian law, *supra* note 10 will mean globally operating (US) service providers will be faced with two directly conflicting laws: they will be asked to prevent access by foreign LEAs, while remaining under an obligation in the US to provide access to this data if it is within their 'control', as the *Microsoft Warrant* case showed. This may mean service providers will have to choose whether to abandon offering its services within Russia by preventing its site from being accessible there, or sever its corporate structure so that Russian data is inaccessible to its parent company.
[16] Transborder Group 'Tranborder Access to Data and Jurisdiction: Options for Further Action by the T-CY' (T-CY 2014 16, 3 December 2014), para. 3.2.

investigations",[17] yet the US offices handling MLA requests have "had flat or reduced funding over time."[18] Certainly, if MLA worked efficiently and effectively and could better meet the needs of the LEA communities, many of the current difficulties would fall away: service providers would no longer be placed in the position of having to assess the validity of foreign requests; sovereignty concerns would be lessened as providers would not be approached directly; and enforcement capabilities would be more distributed.

There are, however, numerous barriers to this being resolved in the immediate future, or ever being the whole solution. First, the tardiness of MLA across the world means performance standards are uncertain, and therefore the present risk of reputational harm from delay is little.[19] Second, if MLA requests are sent to the place where the provider is established,[20] this currently places a disproportionate burden on the US to respond to these requests, given the density of service providers there. The US will be slow to expedite its domestic processes as it would bear the brunt of the costs for improving access to data, without seeing any immediate, reciprocal gains. There would certainly be long-term benefits: it would reduce the need for data sovereignty laws, thus allowing the US to further its vision of a "free and open Internet";[21] it would likely maintain the dominance of US service providers; and most importantly, it would improve global policing capabilities, thus reducing cybercrime worldwide. But these indirect benefits require some foresight, and it may not be clear at present that what is gained "is larger than what they invest."[22] Moreover, routing requests through States, rather than directly to service providers, will undoubtedly decrease the efficiency and speed of current practices.

---

[17] 'Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies' (12 December 2013), 227, available at: http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (Accessed 20/12/2014).
[18] Ibid, 228.
[19] See discussion of Guzman, chapter three, section 3.3.
[20] If, following the *Microsoft Warrant* case, consensus forms that requests should be sent to the place where the data is located, this may render responses even more time-consuming and protracted, as LEAs would first have to contact the State where the service provider is located, in order to establish where the data is, and then send a further request to the country where the data is stored.
[21] See recent comments by President Obama: http://www.cnet.com/uk/news/president-obama-calls-on-fcc-to-keep-internet-free-and-open/ (Accessed 20/12/2014).
[22] Guzman (2008), 12.

States are therefore at a crossroads. They need to either drastically overhaul formal inter-State assistance,[23] or they need to make further provision for direct transnational access to foreign service providers. The latter option itself entails two choices: *supplementing* current networks, or *subsuming* the networks.

9.2.1. Supplementing Networks

The first option is to further formalise the networking interactions between LEAs and service providers so as to remedy current deficiencies (e.g. namely that these relationships can be ad-hoc, insecure, and unreliable, particularly with less prominent providers). This will be the most tempting option for States like the UK who already have a collaborative relationship with many service providers; it would allow domestic LEAs to build upon the flexible and functional *status quo*. Proposals have already emerged from a UK law enforcement officer to do precisely this.[24] Kent proposes LEA-to-industry interfaces based on current practices between UK LEAs and service providers like Facebook.[25] Interactions would be based on standardised submission forms, single points of contact between the requesting LEA and provider, and communication would only be done through secure interfaces. Initially, the system would be restricted to "subscriber data"[26] in order to secure "maximum buy-in",[27] with the hope that it would eventually be scaled up to include traffic data, and even content.[28] Governance and oversight mechanisms are specifically envisaged.[29]

This attempts to impose forms of global administrative standards[30] on the networking interactions between LEAs and service providers, but there are two main difficulties with this course being pursued. First, it would inevitably continue to mean that access to these providers is "unevenly distributed"[31] with

[23] An example of how this could be done was noted in chapter three, note 24: the European Investigations Order. However, as discussed, application of the mutual recognition principle, outside the EU, will not be an easy task.
[24] Kent (2014).
[25] Ibid, para. 67.
[26] This is defined at ibid. para. 76 although there are a diversity of interpretations of subscriber data in practice. See Council of Europe Report 'Rules on Obtaining Subscriber Information' (T-CY 17, 3 December 2014), para. 2.3.1.
[27] Kent (2014), para. 59.
[28] Ibid, para. 62.
[29] Ibid, paras. 92-102.
[30] Kingsbury, Krisch, and Stewart (2005).
[31] Raustiala (2002), 16.

"restricted participation."[32] Kent recognises that due to the divergences in human rights standards across the world, direct access to the system would have to be restricted to the "'five eyes' countries and/or the European Union."[33] Other countries would have to route their requests through Interpol, who would act as an authenticator, checking whether they meet requirements.[34] It is not clear how the latter could operate in practice.

The second problem with supplementing networks is that there are fundamental human rights concerns with this being dealt with outside of legally binding frameworks and oversight mechanisms. Moreover, service providers, established within the EU at least, will not be able to comply with their data protection obligations if they are voluntarily responding to foreign requests.[35] This could be met by participating States adopting extraterritorial procedural powers, such as those found in the DRIP Act 2014.[36] However, as I argued, this would entail not only the extraterritorial prescription of laws, but also their extraterritorial enforcement.

Therefore, expanding, formalising, and supplementing current transnational interactions between LEAs and service providers is either going to require transforming concepts of international law (in particular the meaning of extraterritorial enforcement jurisdiction and the principle of non-interference), or transforming data protection law, or, more likely, both.

9.2.2. Subsuming Networks

The second option for States, if they seek to further regularise direct transnational access to foreign service providers, is to subsume the process explicitly within the Convention or a separate international treaty. Article 32(b) is not the answer here. As I argued in chapter four, this provision was not designed—and is not equipped—for these transnational interactions, despite how it is presently being interpreted in the Transborder Group's Guidance Note and

[32] Eilstrup-Sangiovanni (2009), 202.
[33] Kent (2014), para. 57. The 'five eyes' refers to the close intelligence alliance that exists between the US, the UK, New Zealand, Australia, and Canada.
[34] Ibid, para. 73.
[35] See chapter four, section 4.2.2.3.
[36] See chapter four, section 4.2.2.1.

beyond. These interpretations are contributing to the current paradigm whereby LEAs have a guise of legality for their interactions with foreign service providers, who in turn decide with which countries they will 'voluntarily' cooperate, and when.[37] This helps to create the relatively narrow LEA 'club' that can effectively conduct cybercrime investigations, and also hampers one of the strategic objectives of the Convention—widespread ratification[38]—as countries like Russia are well known to have refused the Council of Europe's invitation to ratify it, due to Article 32(b).

A clear and explicit formal framework for these transnational interactions such as that proposed by Kent, but agreed to by States in a binding legal instrument, would obviously bring many benefits by clarifying service providers' obligations, reducing asymmetries, and distributing enforcement capabilities. But there are again huge barriers to subsuming these networks formally in this way. First, policing superpowers will have little incentive to do so, as they presently have considerable access. Formalisation in a treaty would also likely reduce the effectiveness of current relationships, as States would have to compromise and agree the circumstances where such interactions can occur. The costs of formalisation could, therefore, be seen to outweigh the gains of current informal collaborative efforts. Second, for all States concerned, this would involve drastic relinquishments of sovereignty, as it would allow other States that are a party to the agreement to enforce their laws on service providers in other territories. One can imagine the idea of an autocratic regime being permitted to contact UK service providers directly for data about UK citizens not being a very palatable prospect in Westminster.

9.2.3. A Double-edged Sword

As can be seen, there are no easy choices. The interim period is likely to entail further 'voluntary' cooperation between service providers and LEAs. The future demands further research dedicated to finding more formal, internationally agreed mechanisms, with adequate safeguards, oversight, and respect for human rights. A more comprehensive study focused directly on this issue is needed, and

[37] It will be recalled that the provision requires the 'lawful and voluntary consent' from the person providing the data.
[38] Rozensweig (2012), 420. See also Goldsmith (2011).

rational choice theory could assist to determine the possibilities. Overhauling the way MLA operates, or finding mechanisms that would transcend MLA, is imperative for the future of cybercrime policing. It is inevitable that States will ultimately find further ways of improving transnational access to extraterritorial data, and while this is a necessary and laudable objective, it is also a double-edged sword. It will necessarily mean that more States have the capacity to investigate and pursue transnationally operating cybercriminals. The problem of jurisdictional concurrency over cybercrime will, therefore, be an issue that will only increase in the future, and the next section considers some of the ways that States need to respond to this inevitability.

9.3 Addressing Jurisdictional Concurrency

One of my central claims in this thesis has been that the malleability of the concept of territoriality, and the ease with which States can claim territorial jurisdiction over a cybercrime, has been an insidious development, and generates a problem of jurisdictional concurrency on a hitherto unseen scale. Existing accounts in the literature of how jurisdictional concurrency should be addressed were found to be ill-equipped to deal with this new phenomenon.[39] These complexities cry out for a straightforward solution such as, for example, a jurisdictional prioritisation of the State where the offender was when the crime was initiated. But there are no such easy remedies to the issue of concurrent jurisdiction. States will never agree to a complete subjugation of one or other of the objective or subjective principles of territoriality,[40] while other quick fixes, such as a prioritisation of nationality jurisdiction, would be normatively problematic.[41]

The advent of the web generated some initial speculation about the development of a-territorial concepts for regulating Internet activities,[42] but these have not eventuated, and are not on the horizon in any shape or form in the immediate future. It may be that the "territorially focused criminal law is … moving

[39] See discussion of Ryngaert and Luchtman in chapter two, section 2.6.
[40] See chapter two, and chapter five, section 5.5.
[41] See chapter two, section 2.5.1.
[42] See e.g. Johnson and Post (1996) on a "decentralised, emergent law."

towards tipping point",[43] but it is not clear what it is tipping towards. We appear to be stuck with territoriality as the main jurisdictional principle for regulating cybercrime, and once we resign ourselves to this inevitability for the foreseeable future, it highlights the pressing need to find mechanisms to build jurisdictional reasonableness into current inter-State processes and specifically, I argue, the work of TGNs.

9.3.1. More Choices

The complexities of cybercrime investigations and prosecutions have expectedly led to calls for the globalisation of law enforcement, and the creation of an international criminal court for cybercrimes, with an international prosecutor.[44] Slaughter's concept of the "globalisation paradox",[45] elucidates why this is also an unforeseeable prospect. While we live in a time where a whole host of problems points to the need for these issues to be addressed on a global scale, attempts to locate power above the State face staunch resistance in the current international system. With discussions on-going for the creation of an EU Prosecutor's Office, it cannot of course be discounted that this form of criminality—which is unprecedented in terms of its complexity and multijurisdictionality—will result in some form of international prosecutorial system that could obviate many of the arising territorial conundrums. However, we are a long way from conditions being conducive for this to occur.

Another option that is sometimes touted as a potential means for addressing the fact that we are "increasingly confronted with situations where two or more … States have jurisdiction to investigate and bring to trial the same or related criminal offences … e.g. cyber attacks",[46] is agreement on the formal transferal of criminal proceedings. Such an instrument was recently proposed in the EU based on a Council of Europe Convention,[47] despite the latter being very rarely

[43] Kohl (2007), 106.
[44] Schjolberg (2014).
[45] Slaughter (2004), 8-10.
[46] Explanatory Report to the Draft Council Framework Decision on the transfer of proceedings in criminal matters, (Council Doc. 111119/09, 3 July 2009). Available at: http://www.statewatch.org/news/2009/jul/eu-council-trans-proceedings-em-11119-add1.09.pdf (Accessed 20/12/2014).
[47] European Convention on the Transfer of Criminal Proceedings (CETS No. 073, 15 May 1972).

used,[48] and not widely ratified.[49] This would allow one State to ask another State to take over proceedings when, for example, the suspect is a national or resident of the State, or because evidence or victims are located there.[50] Again, I am pessimistic of this assisting very much. First, these decisions are already made informally by TGNs of investigators and prosecutors, and it is not clear how such an instrument would assist with the *status quo*. Second, the latest discussion actually advocated *extending* jurisdictional grounds even further, in order to cater for situations where the requested State cannot prosecute under any traditional jurisdictional principles.[51] I believe I have already established that States have adequate jurisdictional scope for bringing prosecutions against cybercrimes, and extending jurisdictional grounds could hardly ameliorate the problems arising from jurisdictional concurrency, which is what the EU proposal was meant to do.

This all points to the work of TGNs continuing to be the crucial area for focus in developing jurisdictional reasonableness. Decisions between TGNs will often be determinative as to place of prosecution and one of the findings of this thesis, in my investigation of the work of these actors, has been that the multitude of factors that need to be taken into account in these decisions[52] make it impossible to create any bright line rules that will provide clear-cut jurisdictional answers.[53] Nevertheless, I have also shown that in this disaggregated state system of transgovernmental cooperation there is a distinct danger of jurisdictional normativity being lost in the mechanics of a decentred opaque cluster of networking law enforcement actors. Viewed only from the perspective of enforcement this may not appear to be of any great significance: what matters from this point of view is that criminals are prosecuted, not where it is done.

---

[48] Eurojust Interview.
[49] Only 25 States have ratified the Convention.
[50] See Article 7 of 'Proposal for a Council Framework Decision on the Transfer of Proceedings in Criminal Matters. (Council Doc. 14934/09, 28 October 2009).
[51] See Article 5 ibid, and the proposed introduction of "subsidiary jurisdiction" (for discussion, ibid, para. 5). The Presidency suggested that "[a]ll Member States should, for the purpose of applying an instrument on transfer of proceedings, to some extent *be obliged to extend their national rules on jurisdiction* to include other offences committed outside the territory of their Member State. This would contribute to the fight against cross border crime." Presidency Note, 'Draft […] on Transfer of Proceedings in Criminal Matters' (Council Doc. 16437/09, 24 November 2009), para. 13. Emphasis added.
[52] See chapter six.
[53] This is why I don't see the development of a matrix that would score all of the relevant factors on a scale—making jurisdictional determination an almost mathematical equation—as a possibility. For a suggestion to this end, see Vermeulen, Bondt, and Ryckman (2012), 38-9.

However, I have shown that there are a number of dangers with adopting this myopic philosophy. First, it can generate inter-State conflict, as demonstrated in chapter seven, which could prompt States to revert to uncooperative tools, such as bars to extradition based on a suspect's nationality. Second, it can dis-incentivise capacity building as some States free ride and externalise the costs of law enforcement. Third, there is significant potential for unfairness for the accused: he may be prosecuted in a foreign justice system without the resources he may have had to defend himself in his home country; he could be incarcerated far from home and family for periods of time that could be vastly longer than he would have faced if prosecuted domestically;[54] and he may even be re-prosecuted repeatedly for the same acts.

There are a number of direct and indirect tools that could be used to further embed jurisdictional reasonableness within TGNs, and I see the suppression project as providing an important avenue for their promotion.

9.3.2. Development of Cybercrime-specific Guidelines for TGNs

In most other areas of transgovernmental cooperation there are significant efforts to implement accountability mechanisms, such as enhancing the transparency of decision-making (e.g. notice-and-comment procedures) or promotion of judicial review.[55] Given the sensitivity of criminal investigations, however, much of this movement will be unsuitable for transposition into the negotiations of TGNs (e.g. publication of jurisdictional determinations).

Nevertheless, the development of guidelines for cybercrime jurisdictional negotiations could assist to introduce further accountability and standards for these determinations. Such guidelines could be prepared by the Council of Europe, so as to supplement the consultation provision found in Article 22(5) of the Convention. The Eurojust Guidelines, discussed in chapter six, would be instructive, but could be improved upon. The interests of the accused and his connections with a particular State could be specifically enumerated as requiring

[54] Work should also be done to consider how regimes around the transfer of sentenced persons—such as the CoE Convention on the Transfer of Sentenced Persons—could be improved, but this has been outside the scope of the present thesis.
[55] For discussion of the globalisation of administrative law, see Esty (2005) and Kingsbury, Krisch, and Stewart (2005).

consideration. It could also create a hierarchy of jurisdictional bases, prioritising territoriality,[56] but the specificities and complexities of cybercrime demand a more granular approach: the general presumption that prosecutions should ordinarily be brought where most of the criminality occurred or where most of the harm or loss occurred, could be interpreted broadly to mean, in the case of content offences for example, that most of the criminality occurs in the place where the servers are located—a jurisdictional interpretation of territoriality which I have critiqued at some length.[57] A more granulated approach could be taken which could attempt to unpack the concept of territoriality. Weak forms of territorial jurisdiction could be highlighted, such as prosecutions based only on the accessibility of a website, without any form of targeting. Presumptions could then be created which would deter some of the tenuous jurisdictional seizures which I described in chapter seven. For example, it could state that where a State's only connection with an offence is that content is accessible within that jurisdiction, or that the content was stored remotely there, the place where the accused was acting from would be presumed to be the more appropriate forum.

While such guidelines could serve to stimulate jurisdictional reasonableness and further harmonise interpretations of territoriality, my interview findings would suggest that TGNs may not, in practice, rely on them very heavily.[58] A more promising—but indirect—way of ensuring that broader factors of relevance are taken into account when prosecutors and police meet "behind closed doors"[59] would be to pay closer attention to extradition processes. I argue that the interests of States, individuals, and the long-term prospects of the suppression project, would be promoted through the adoption of two particular extradition bars: a forum bar, and a *ne bis in idem* bar.

[56] Nationality jurisdiction, as discussed in chapter two, is a normatively questionable jurisdictional ground, but it is unlikely that States will—in the near future—be willing to relinquish their authority to prosecute on this base, or to excise it from Article 22(1)(d) of the Convention.
[57] See discussion in chapter five, section 5.5, and chapter seven, section 7.5.
[58] See chapter six.
[59] Home Affairs Committee 'The US-UK Extradition Treaty' (2012), para. 32.

9.3.3. A Forum Bar in Suppression Conventions

While this thesis has pointed to the importance of the work of TGNs in jurisdictional determinations, it has also highlighted the importance of extradition law in determining which country ultimately prosecutes. Given the continued rigidity of the "public law taboo"[60]—the fact that courts are averse to applying the criminal law of other countries—extradition hearings are essentially the only venue for forum determinations. Judges are shackled if the only opportunity they have to comment on forum is when the accused is before them for prosecution. Even if the jurisdictional grounds for prosecution are weak in the case, the LEAs of the country concerned may have invested significant time and money, particularly if extradition has been involved, and it is unrealistic to expect that the court would refuse to hear the prosecution at that stage when there is some territorial link. However, I have also shown that the trajectory of extradition law can be to circumscribe judicial discretion so as to prevent forum determinations in cases of jurisdictional concurrency.[61] Promoting the adoption of a forum bar to extradition—such as has been developed in the UK—through the extradition provisions of suppression conventions, would have a profound impact as it would provide judiciaries with the opportunity to develop jurisprudence on jurisdictional concurrency, which has been sorely lacking. A further benefit is that it would stimulate more careful consideration of these normative considerations within TGNs; investigators will be less likely to aggressively pursue extraditions if it is known that the courts will address the issue of forum in extradition proceedings, and are more likely to work collaboratively with their counterparts.

There are, of course, dangers and drawbacks, most notably, that it will elongate extradition proceedings. It may also be feared that judges will 'pull for the home crowd' and that it may result in impunity for cybercriminals, due to evidential challenges in transferring evidence and securing witness attendance from the investigator's jurisdiction. And an even broader challenge will be to convince States that a forum bar should be promoted through a suppression convention, as it would buck the LEA-oriented nature of these instruments, which have only

[60] See Lowenfeld (1979), 322-6 for discussion.
[61] See chapter seven, section 7.4.

ever attempted to remove obstacles to extradition, rather than suggest their imposition. Rational self-interested States would also likely prefer to introduce forum bars domestically to prevent their citizens from being extradited on tenuous grounds, but not to advocate wider adoption as it would delay their own extradition requests to foreign States.

These are certainly formidable barriers to the promotion of forum bars. However, my thesis has provided sufficient countervailing considerations to suggest that the broader benefits may outweigh these concerns. Impunity should not eventuate, as States remain bound by *aut dedere aut judicare* obligations, such as in Article 24(6) of the Convention. Improvements will be needed in processes for evidence transfer and the ability to provide witness testimony remotely (e.g. video-conferencing), but in the 21st century this should not prove insurmountable, and more efforts should be focused on this regardless. It will also incentivise capacity building so that more States are equipped to prosecute domestic offenders.

There will be challenges in promoting forum bars through suppression conventions, rather than simply letting States develop such bars unilaterally when they are faced with the jurisdictional concurrency problems which developed in the UK. But the risk in the unilateral approach is that these States will then revert to nationality bars, or other uncooperative practices. A very basic starting point could be a provision which would simply state that a State has the right to refuse extradition if there has been a judicial determination that it is the more appropriate forum for prosecution. This should not appear particularly revolutionary,[62] but as we saw in the context of UK extradition law, may not currently be an option in some countries. It should be promoted as a judicial bar, rather than a general discretion for the executive, so that the international community can benefit from reasoned decisions on forum, allowing

[62] Article 4(7)(a) of the European Arrest Warrant Decision recognises, for example, that States can refuse execution of a request if the offence was "committed in whole or in part in its territory." See also Article 7(1) of the European Extradition Convention, and Article 2(3) of the Inter-American Convention on Extradition (*supra* chapter seven, note 92). These provisions do not, however, invite determinations on forum, but rather re-iterate that requested States could simply blankly refuse to extradite an individual, even if they have a much weaker territorial case than the requesting State.

jurisdictional reasonableness to "come into being."[63] Encouraging States to agree on an un-weighted list of factors such as that found in section 19B of the Extradition Act 2003 will be a more daunting challenge, but is a worthy area for further research. A study that would document the operation of the forum bar in the UK, may assist to further internationalise their use and adoption in international suppression conventions.

9.3.4. Ne Bis in Idem

In chapter eight I argued that the multijurisdictional nature of cybercrime demands that attention be given to further international agreement on the concept of *ne bis in idem* applying between States, and critiqued the doctrine of dual sovereignty. Amendment of international human rights instruments such as the ECHR, the American Convention on Human Rights, and the International Covenant on Civil and Political Rights, must be considered to this end. I acknowledged, however, that the lack of procedural harmonisation in criminal justice systems will make this another daunting endeavour.

An indirect, but less challenging, method of generating further consensus on this topic is again to turn to the extradition process, as one of the key venues where the principle could be considered and applied. Some extradition agreements already state that extradition should not occur if it would constitute a breach of the *ne bis in idem* principle, such as Article 9 of the European Convention on Extradition.[64] However, this and other extradition agreements, adopt a legal classificatory approach to *idem* – they only prohibit extradition if there has been a final judgment for the same *offence*.[65] As has been recognised by the ECtHRs and the CJEU this approach does not adequately protect the rights of the individual.[66] Moreover, they limit its application to situations where the individual was prosecuted in the requested State, not where the individual may have been prosecuted in a third State.

---

[63] Ryngaert (2008), 184. See also O'Keefe (2013) on the role which domestic judicial decisions can take in shaping international law concepts on prescriptive and adjudicative jurisdiction.
[64] It is also suggested as a bar in Article 3(d) of the UN Model Treaty on Extradition, GA Resolution 45/116 (14 December 1990).
[65] The suggested extradition bar in the UN Model Treaty on Extradition, ibid, is equally limited.
[66] See chapter eight, section 8.4.

I argue that the suppression project could also be an avenue for securing further inter-State *ne bis in idem* protection for the accused. It is, indeed, an inconsistency that two Council of Europe conventions which both provide for the extradition of individuals do not equally protect the principle as an extradition bar. It cannot be argued that the reason for its non-protection in the Cybercrime Convention is because it is already adequately protected in the Extradition Convention: numerous countries that have ratified the Cybercrime Convention have not ratified the Extradition Convention, and thus may not be bound by the principle in their extradition practices. The more likely reason is that the rights of the accused are not taken into account in this LEA-oriented endeavour.

Therefore, the amendment of the Convention to mandate a *ne bis in idem* extradition bar would also be a step-change. There are also concerns, as there are within the EU, that such a bar will overprotect: by prosecuting a cybercriminal for one aspect of a potentially much wider cybercrime enterprise, authorities could inadvertently prevent the full extent of criminality from being dealt with, and preclude other States from extraditing and prosecuting the individual. Another danger, as the European Commission has observed, is that it will result in an arbitrary 'first come first served' approach in the prosecution of transnational offences.[67] While these are legitimate concerns, they must not be used as an excuse to evade human rights responsibilities. Instead, a *ne bis in idem* extradition bar in the Convention ought to spur the work of TGNs by mandating consideration of forum and the consequences of prosecution, from the outset. The test of the CJEU on 'same acts' will also be instructive for judges considering *ne bis in idem* in extradition cases, and is the most appropriate tool to strike the difficult balance between preventing unfairness to the accused by repeated prosecutions, and stymieing prosecutions for distinct acts. It will obviously not prevent States from re-prosecuting an individual for the same acts if they are arrested whilst travelling through their territory. But it would serve as an important catalyst for developing further international consensus on *ne bis in idem*, and provide significantly more protection to the accused than is currently available in international law and extradition agreements. As argued in the

[67] Commission Staff Working Document, 'Annex to the Green Paper on Conflicts of Jurisdiction and the Principle of ne bis in idem in Criminal Proceedings' (COM 696 final, 2005), 3.

previous chapter, efforts must also be orientated towards developing further consensus on all elements of the *ne bis in idem* principle in international law, and more research is needed to this end.

9.4 Conclusion

Difficulties are inherent in any multilateral project. They involve cumbersome negotiations and high transaction costs. Potential cooperative outcomes are always tempered by the diversity of the States involved, and many see the entire suppression project as one which "oozes Western bias because of Western domination over the making of international law."[68] But the suppression project and the traditional State-based system of policing have been confronted with unique challenges with the advent of cybercrime. While I have argued that there has been a lack of analytical balance by commentators who contend that cybercrime is resulting in a decline of the Nation State and a 'loss of control',[69] I am not assuming that cybercrime enforcement is in any way currently 'under control' or effective. Cybercrime is unique in the history of transnational crimes due to its multijurisdictional and multi-victim nature. It has never been so complicated and difficult for law enforcement to police a transnational crime, and the threat is likely only to increase in sophistication and prevalence in the future. The de-centralised State-based system of policing, upon which multilateralism is predicated, will always undoubtedly struggle to respond to this. As Kim Dotcom has said, "you can't stop a river with your bare hands. Water just flows around them."[70] I am sure this is exactly how many investigators feel when attempting to unilaterally pursue a cybercrime investigation.

The Cybercrime Convention also faces ratification challenges, with key countries that are widely seen to be 'cybercrime havens'[71] abstaining from participation. This is a result of a number of factors, including the difficulty of acceding to the

[68] Ryngaert (2008), 201.
[69] See chapter one, section 1.1.
[70] http://www.theguardian.com/technology/2013/may/04/security-alert-war-in-cyberspace (Accessed 20/12/2014).
[71] Labelling Russia as a 'haven', as Brenner (2014), 55 does, ignores a reality that is seldom acknowledged or discussed: it is the US that actually tops the list of most threat reports as the source of most malicious activity. Symantec 'Internet Security Threat Report', Appendix, (2014), 8.

Convention,[72] and a general wariness from States of ratifying an instrument when they were not involved in its development or negotiation. This may well, in the long term, require a return to the negotiating table for a new UN convention on cybercrime, although I foresee the Cybercrime Convention having a strong potential to endure given its backing by countries such as the US and the UK.

These challenges have caused many to lose faith in the utility of the suppression project for countering cybercrime. But I believe it will continue to have a role to play, and this contention is based on the following assumptions. First, the State is a construct that is not in any immediate danger of extinction. Second, it will retain, for the foreseeable future, "the monopoly of the legitimate use of physical force",[73] and the enforcement of criminal laws will remain within its exclusive preserve. Third, the basic two-fold strategy[74] behind suppression conventions remains coherent, even if more difficult to implement in the case of cybercrime.

This being said, I do not see suppression conventions in any way to be the "holy grail"[75] for dealing with cybercrime. There is a limit to the role that States can play in tackling cybercrime and the "gap is … filled by other methods."[76] Countering this criminality will, as Shackleford notes, involve a "mixture of laws and norms; market-based incentives; code; self-regulation; public-private partnerships; and bilateral, regional, and multilateral collaboration to enhance cyber-security."[77] The reason why the world is not falling apart around our ears is precisely because we already have these multiple sites of governance in operation, with varying degrees of effectiveness. I see multilateralism, therefore, as only one cog in the fight against cybercrime, albeit an important one which cannot simply be dismissed offhand because of current ratification challenges.[78] This requires that we pay close attention to the development of this suppression project. This thesis has charted the current jurisdictional trajectories and imbalances, and their implications for States and individuals. I hope to have

[72] Article 37 requires that any invitation to accede to the Convention to a State which is not a member of the Council of Europe must have the unanimous consent of the Contracting States.
[73] Weber (1948), 78.
[74] See chapter three.
[75] Kohl (2014).
[76] Mueller (2010), 162.
[77] Shackelford (2014), 342.
[78] See e.g. Brenner (2014), 96.

elucidated and clarified some of the choices confronting States if they are to attempt to re-balance the jurisdictional scales.

Bibliography

ABEL, W. & SCHAFER, B., 'The German "Federal Trojan": Challenges between Law and Technology', *Teutas Law and Technology*, 17 (2009) 48.

ABELSON, A., 'The Prosecute/Extradite Dilemma: Concurrent Criminal Jurisdiction and Global Governance', *UC Davis Journal of International Law and Policy,* 16(1) (2009), 1.

ADAM, A., 'What is "Commercial Scale"? A Critical Analysis of the WTO Panel Decision in WT/DS362/R', *European Intellectual Property Review*, 33:6 (2011) 342.

AKDENIZ, Y., *Internet Child Pornography and the Law: National and International Responses,* (Ashgate: 2008).

AKEHURST, M., 'Jurisdiction in International Law', *British Yearbook of International Law,* 46 (1972-3), 145.

ALLDRIDGE, P., 'Threats Offences: A Case for Reform', *Criminal Law Review*, (1994) 176.

ALVAREZ, J., 'Multilateralism and its Discontents', *European Journal of International Law,* 11 (2000), 393.

ALVAREZ, J., 'Do Liberal States Behave Better? A Critique of Slaughter's Liberal Theory', *European Journal of International Law,* 12 (2011), 183.

AMSTERDAM, R. & ROTHKEN, I., 'Megaupload, the Copyright Lobby and the Future of Digital Rights: The United States vs You (and Kim Dotcom)', *White Paper* (2013), <http://www.kim.com/whitepaper.pdf> (Accessed 20/12/2014).

ANDREAS, P., 'Illicit Globalization: Myths, Misconceptions, and Historical Lessons', *Police Science Quarterly,* 126(3) (2011), 403.

ANDREAS, P., *Smuggler Nation: How Illicit Trade Made America,* (Oxford University Press: 2013).

ANDREAS, P. & NADELMANN, E., *Policing the Globe: Criminalization and Crime Control in International Relations*, (Oxford University Press: 2006).

ANSLINGER, H. & TOMPKINS, W., *The Traffic in Narcotics*, (Funk & Wagnalls: 1953).

ARNELL, P., 'The Case for Nationality Based Jurisdiction', *International and Comparative Law Quarterly,* 50 (2001), 955.

BAILEY, S., *The Anti-Drug Campaign: An Experiment in International Control*, (King & Son: 1935).

BANISAR, D. & HOSEIN, G., 'A Draft Commentary on the Council of Europe Cybercrime Convention', (2000), <http://privacy.openflows.org/pdf/coe_analysis.pdf >, (Accessed 20/12/2014).

BARLOW, J.P., 'A Declaration of Independence of Cyberspace', (1996), <https://projects.eff.org/~barlow/Declaration-Final.html> (Accessed 20/12/2014).

BARTLETT, J., *The Dark Net: Inside the Digital Underworld*, (William Heinemann: 2014).

BASSIOUNI, M.C., *International Extradition and World Public Order*, (Oceana Publications: 1974).
BASSIOUNI, M.C. (ed.), *International Criminal Law,* 3rd ed., (Martinus Nijhoff Publishers: 2008).
BASSIOUNI, M.C., *Introduction to International Criminal Law*, (Martinus Nijhoff Publishers: 2012).
BASSIOUNI, M.C., *International Extradition: United States Law and Practice*, (Oxford University Press: 2014).
BECCARIA, C., *An Essay on Crime and Punishments*, CASO A., (ed), 4th ed, (International Pocket Library: 1992).
BEDI, S. D., *Extradition in International Law and Practice*, (Bronder-Offset: 1966).
BELFIORE, R., 'The Protection of Personal Data Processed Within the Framework of Police and Judicial Cooperation in Criminal Matters'. *In:* RUGGERI, S. (ed.), *Transnational Inquiries and the Protection of Fundamental Rights in Criminal Proceedings,* (Springer: 2013).
BELLIA, P., 'Chasing Bits Across Borders', *The University of Chicago Legal Forum,* (2001), 35.
BERG, B. & LUNE, H., *Qualitative Research Methods for the Social Sciences*, (Pearson: 2012).
BERNARD, D., 'Ne Bis In Idem: Protector of Defendants' Rights or Jurisdictional Pointsman?', *Journal of International Criminal Justice,* 9(4) (2011), 863.
BESSON, S. & TASIOULAS, J. (eds.), *The Philosophy of International Law* (Oxford University Press: 2010).
BIGO, D., 'Liaison Officers in Europe: New Officers in the European Security Field'. *In:* SHEPTYCKI, J. (ed.), *Issues in Transnational Policing,* (Routledge: 2000).
BINNING, P. & CAMPBELL, D., 'No Forum for Debate on Extradition', *The Law Society Gazette*, (2008),<http://www.lawgazette.co.uk/4539.article>, (Accessed 20/12/2014).
BLAKESLEY, C., 'Extraterritorial Jurisdiction. *In:* BASSIOUNI, C. (ed.) *International Criminal Law,* 3rd ed, (Martinus Nijhoff Publishers: 2008).
BLAKESLEY, C. & LAGODNY, O., 'Finding Harmony Amidst Disagreement Over Extradition, Jurisdiction, The Role of Human Rights, and Issues of Extraterritoriality Under International Criminal Law', *Vanderbilt Journal of Transnational Law,* 24(1) (1991), 1.
BLOCK, L., 'Bilateral Police Liaison Officers: Practices and European Policy', *Journal of Contemporary Research,* 6(2) (2010), 194.
BLOCK, L., 'EU Joint Investigation Teams: Political Ambitions and Police Practices'. *In:* HUFNAGEL, S., HARFIELD, C. & BRONITT, S. (eds.), *Cross-Border Law Enforcement: Regional Law Enforcement Cooperation - European, Australian and Asia-Pacific Perspectives,* (Routledge: 2012).
BLUM, G., 'Bilateralism, Multilateralism, and the Architecture of International Law', *Harvard International Law Journal,* 49(2) (2008), 323.
BOCKEL, B.V., *The Ne Bis in Idem Principle in EU Law*, (Kluwer Law International: 2010).
BOISTER, N., 'Transnational Criminal Law?', *European Journal of International Law,* 14(5) (2003), 953.

BOISTER, N., *An Introduction to Transnational Criminal Law*, (Oxford University Press: 2012).

BOISTER, N. & CURRIE, R. (eds.), *Routledge Handbook of Transnational Criminal Law*. (Routledge: 2014) .

BRADSHAW, S., MILLARD, C. & WALDEN, I., 'Contracts for Clouds: A Comparative Analysis of Terms and Conditions for Cloud Computing Services', *International Journal of Law and Information Technology,* 19(3) (2011), 187.

BRENNAN, F., 'Legislating *against* Internet Race Hate', *Information and Communications Technology Law,* 18(2) (2009), 123.

BRENNER, S., 'The Next Step: Prioritizing Jurisdiction. *In:* KOOPS, B.-J. & BRENNER, S. (eds.), *Cybercrime and Jurisdiction – A Global Survey,* (Springer: 2006).

BRENNER, S., 'Law, Dissonance, and Remote Computer Searches', *North Carolina Journal of Law & Technology,* 14(1) (2012), 43.

BRENNER, S., 'Remote Computer Searches and the Use of Virtual Force', *Mississippi Law Journal,* 81(5) (2012), 1229.

BRENNER, S., 'Cyber-threats and the Limits of Bureaucratic Control', *Minnesota Journal of Law, Science & Technology,* 14(1) (2013), 137.

BRENNER, S., *Cyberthreats and the Decline of the Nation-State*, (Routledge: 2014).

BRENNER, S. & SCHWERHA, J., 'Transnational Evidence Gathering and Local Prosecution of International Cybercrime', *John Marshall Journal of Information Technology and Privacy Law,* 20(3) (2002), 347.

BRETON, A. (ed.), *Multijuralism: Manifestations, Causes, and Consequences,* (Ashgate: 2009).

BREWSTER, R., 'Unpacking the State's Reputation', *Harvard International Law Journal,* 50 (2009), 231.

BRONITT, S., 'Shifting Paradigms: Jurisdiction and Criminal Justice Cooperation in the Shadow of Law'. *In:* HUFNAGEL, S., HARFIELD, C. & BRONITT, S. (eds.) *Cross-Border Law Enforcement: Regional Law Enforcement Cooperation - European, Australian and Asia-Pacific Perspectives,* (Routledge: 2012).

BROOKSON-MORRIS, K., 'Conflicts of Criminal Jurisdiction', *International and Comparitive Law Quarterly,* 56(3) (2007), 659.

BRUUN, K., PAR, L. & NORVAL, M., *The Gentlemen's Club: International Control of Drugs and Alcohol (Studies in Crime and Justice Series)*, (University of Chicago Press: 1975).

BUNYAN, T., 'Trevi, Europol and the European state'. *In:* BUNYAN, T. (ed.), *Statewatching the New Europe: A Handbook on the European State,* (Statewatch: 1993).

BUNYAN, T. (ed.), *Statewatching the New Europe: A Handbook on the European State,* (Statewatch: 1993).

BUNYAN, T. (ed.), *Key Texts on Justice and Home Affairs in the European Union: Volume 1 (1976-1993) From Trevi to Maastricht,* (Statewatch: 1997)
<http://www.statewatch.org/semdoc/assets/files/keytexts/ktch5.pdf>
(Accessed 20/12/2014).

BUXBAUM, H., 'Territory, Territoriality, and the Resolution of Jurisdictional Conflict', *American Journal of Comparative Law,* 57 (2009), 631.

CANNIZZARO, E. (ed.), *The Law of Treaties Beyond the Vienna Convention,* (Oxford University Press: 2011).
CASSESSE, A., *International Criminal Law*, (Oxford University Press: 2003).
CHANG, J., 'An Analysis of Advance Fee Fraud on the Internet', *Journal of Financial Crime,* 15(1) (2008), 71.
CHATTERJEE, S., *Legal Aspects of International Drug Control*, (Martinus Nijhoff Publishers: 1981).
CHEHTMAN, A., *The Philosophical Foundations of Extraterritorial Punishment,* (Oxford University Press: 2010).
CHOO, K.K., SMITH, R. & MCCUSKER, R., 'Future Directions in Technology-enabled Crime: 2007-09'. *Research and Public Policy Series No. 78*, (2007) Australian Institute of Criminology.
CLAES, E., DEVROE, W. & KEIRSBILCK, B. (eds.), *Facing the Limits of the Law,* (Springer: 2009).
CLARK, R., 'Offenses of International Concern: Multilateral State Treaty Practice in the Forty Years Since Nuremburg', *Nordic Journal of International Law,* 57 (1988), 49.
CLARK, R., 'Jurisdiction over Transnational Crime'. *In:* BOISTER, N. & CURRIE, R. (eds.), *Routledge Handbook of Transnational Criminal Law*. (Routledge: 2014).
CLARKE, E., *A Treatise Upon the Law of Extradition*, (Stevens and Haynes: 1903).
CLOUGH, J., *Principles of Cybercrime*, (Cambridge University Press: 2010).
CLOUGH, J., 'Data theft? Cybercrime and the Increasing Criminalization of Access to Data', *Criminal Law Forum,* 22 (2011), 145.
COCKAYNE, J., 'On the Cosmopolitanization of Criminal Jurisdiction', *Journal of International Criminal Justice,* 3(2) (2005), 514.
COLANGELO, A., 'Double Jeopardy and Multiple Sovereigns: A Jurisdictional Theory', *Washington University Law Review,* 86(4) (2009), 769.
COLLINS, A. (ed.), *Contemporary Security Studies,* (Oxford University Press: 2009).
CONWAY, G., 'Ne Bis in Idem in International Law', *International Criminal Law Review,* 3 (2003), 217.
COOK, W., 'The Application of the Criminal Law of a Country to Acts Committed by Foreigners outside the Jurisdiction', *West Virginia Law Quarterly,* 40 (1934), 303.
COTTIM, A., 'Cybercrime, Cyberterrorism and Jurisdiction: An Analysis of Article 22 of the COE Convention on Cybercrime', *European Journal of Legal Studies,* 2(3) (2010) 1.
CRAWFORD, J., *Brownlie's Principles of Public International Law*, 8th ed, (Oxford University Press: 2012).
CRYER, R., *Prosecuting International Crimes: Selectivity and the International Criminal Law Regime*, (Cambridge University Press: 2005).
CRYER, R. & BEKOU, O., 'International Crimes and ICC Cooperation in England and Wales', *Journal of International Criminal Justice,* 5 (2007), 441.
D'ASPREMONT, J., 'Multilateral Versus Unilateral Exercises of Universal Criminal Jurisdiction', *Israel Law Review,* 43(2) (2010), 301.

DAMROSCH, L., 'Politics across Borders: Nonintervention and Nonforcible Influence over Domestic Matters', *American Journal of International Law,* 83 (1989), 1.
DAVIES, P., 'Accessory Liability for Assisting Torts', *Cambridge Law Journal,* 70(2) (2011), 353.
DEBOYSER, C., 'Eurojust's Role in the Matter of Choice of Forum'. *In:* LUCHTMAN, M. (ed.), *Choice of Forum in Cooperation Against EU Financial Crime,* (Eleven International Publishing: 2013).
DEEN-RACSMÁNY, Z. & BLEKXTOON, R., 'The Decline of the Nationality Exception in European Extradition? The Impact of the Regulation of (Non-) Surrender of Nationals and Dual Criminality under the European Arrest Warrant', *European Journal of Crime, Criminal Law and Criminal Justice,* 13 (2005), 317.
DEEN-RASMANY, Z., 'The European Arrest Warrant and the Surrender of Nationals Revisited: The Lessons of Constitutional Challenges', *European Journal of Criminal Law and Criminal Justice* 14 (2006), 271.
DEFLAM, M., 'Technology and the Internationalization of Policing: A Comparative Historical Perpective', *Justice Quarterly,* 19 (2002), 453.
DENEMARK, R. & HOFFMANN, M., 'Not Just Scraps of Paper: The Dynamics of Multilateral Treaty-Making', *Cooperation and Conflict,* 43(2) (2008), 185.
DEPREEUW, S. & HUBIN, J.B., 'Of Availability, Targeting and Accessibility: Online Copyright Infringements and Jurisdiction in the EU', *Journal of Intellectual Property Law and Practice,* 9(9) (2014), 750.
DOWNS, G., ROCKE, D. & BARSOOM, P., 'Is the Good News about Compliance Good News About Cooperation?', *International Organization,* 50(3) (1996), 379.
DUNN, M., KRISHNA-HENSEL, S. & MAUER, V. (eds.), *The Resurgence of the State: Trends and Processes in Cyberspace Governance,* (Ashgate: 2007).
DUNOFF, J. & POLLACK, M. (eds.), *Interdisciplinary Perspectives on International Law and International Relations,* (Cambridge University Press: 2013).
DYSON, M., 'R. v Sheppard (Simon Guy): Public Order on the Internet', *Archbold Review,* 6 (2010).
EILSTRUP-SANGIOVANNI, M., 'Varities of Cooperation: Government Networks in International Security'. *In:* KAHLER, M. (ed.), *Networked Politics: Agency, Power, and Governance,* (Cornell University Press: 2009).
ENGEL, C., 'States Playing Games', *International Studies Review,* 7 (2005), 328.
ESTY, D., 'Good Governance at the Supranational Scale: Globalizing Administrative Law', *Yale Law Journal,* 115 (2005), 1490.
FARRAR, J., *Crimes and Punishments Including a New Translation of Beccaria's "Dei Delitti E Delle Pene"*, (Chotts and Winders: 1880).
FARRELL, S., YEO, N. & LADENBURG, G., *Blackstone's Guide to The Fraud Act 2006*, (Oxford University Press: 2007).
FASSBENDER, B., 'Sovereignty and Constitutionalism in International Law'. *In:* WALKER, N. (ed.), *Sovereignty in Transition*, (Hart Publishing: 2003).

FEHLINGER, P., 'Cyberspace fragmentation: An Internet Governance Debate Beyond Infrastructure', (2014), <http://policyreview.info/articles/news/cyberspace-fragmentation-internet-governance-debate-beyond-infrastructure/266>, (Accessed 20/12/2014).

FIJNAUT, C. (ed.), *The Internationalization of Police Co-operation in Western Europe*, (Brill: 1993).

FILIPPI, P.D. & MCCARTHY, S., 'Cloud Computing: Centralization and Data Sovereignty' *European Journal for Law and Technology,* 3(2) (2012).

FINKLEA, K., 'The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement', *Congressional Research Service Report* (17 January 2012) <http://www.fas.org/sgp/crs/misc/R41927.pdf> (Accessed 20/12/2014).

GABLE, K., 'Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent', *Vanderbilt Journal of Transnational Law,* 43 (2010), 57.

GALLANT, K., *The Principle of Legality in International and Comparative Criminal Law*, (Cambridge University Press: 2010).

GARCIA, M.J. & DOYLE, C., 'Extradition To and From the United States: Overview of the Law and Recent Treaties', *Congressional Research Service Report*, (17 March 2010), <http://www.fas.org/spg/crs/misc/98-958.pdf>, (Accessed 20/12/2014).

GEISINGER, A. & STEIN, M., 'Rational Choice, Reputation, and Human Rights Treaties', *Michigan Law Review,* 106 (2008), 1129.

GEORGE, B., 'Extraterritorial Application of Penal Legislation', *Michigan Law Review,* 64 (1966), 609.

GIBNEY, M., 'The Extraterritorial Application of US Law: Perversion of Democratic Governance, the Reversal of Institutional Roles, and the Imperative of Establishing Normative Principles', *Boston College International and Comparative Law Review,* 19(2) (1996), 297.

GILL, T., 'Non-Intervention in the Cyber Context'. *In:* ZIOLKOWSKI, K. (ed.), *Peacetime Regime For State Activities in Cyberspace: International Law, International Relations, and Diplomacy,* (NATO Cooperative Cyber Defence Centre of Excellence: 2013).

GILLESPIE, A., 'Racially Offensive Web Postings', *Journal of Criminal Law,* 74 (2010), 205.

GILLESPIE, A., *Child Pornography: Law and Policy*, (Routledge-Cavendish: 2011).

GILMORE, W., *Combating International Drugs Trafficking: The 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*, (Commonwealth Secretariat: 1991).

GILMORE, W., 'International Cooperation in the Administration of Justice: Developments and Prospects', *Commonwealth Law Bulletin,* 18 (1992), 1550.

GILMORE, W., 'Hot Pursuit: The Case of R v Mills and Others', *International and Comparative Law Quarterly,* 44 (1995), 949.

GIRALDO, J. & TRINKUNAS, H., 'Transnational Crime'. *In:* COLLINS, A. (ed.), *Contemporary Security Studies,* (Oxford University Press: 2009).

GLENNY, M., *DarkMarket: Cyberthieves, CyberCops, and You,* (The Bodley Head: 2011).

GOLDSMITH, J., (a) 'Against Cyberanarchy', *The University of Chicago Law Review,* 65 (1998), 1199.
GOLDSMITH, J., (b) 'Regulation of the Internet: Three Persistent Fallacies', *Chicago-Kent Law Review,* 73 (1998), 1119.
GOLDSMITH, J., 'Cybersecurity Treaties: A Skeptical View', Future Challenges Essay, Hoover Institute, Standford University, (2011) < http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf> (Accessed 20/14/2014).
GOLDSMITH, J. & WU, T., *Who Controls the Internet? Illusions of a Borderless World*, (Oxford University Press: 2006).
GOODE, M., 'The Tortured Tale of Criminal Jurisdiction', *Melbourne University Law Review* 21 (1997), 411.
GROTIUS, H., 'De Jure Belli Ac Pacis Libris Tres'. *In:* SCOTT, J.B. (ed.), *The Classics of International Law* (Clarendon Press: 1925).
GRUNDMAN, R., 'The New Imperialism: The Extraterritorial Application of United States Law', *The International Lawyer,* 14(2) (1980), 257.
GUADAMUZ, A., *Networks, Complexity and Internet Regulation*, (Edward Elgar: 2011).
GUZMAN, A., 'The Design of International Agreements', *European Journal of International Law,* 16 (2005), 579.
GUZMAN, A., *How International Law Works: A Rational Choice Theory*, (Oxford University Press: 2008).
GUZMAN, A., 'How International Law Works: A Response to Commentators' *International Theory,* 1(2) (2009), 335.
HACHE, A. & RYDER, N., 'Tis the Season to (be jolly?) Wise-up to Online Fraudsters. Criminals on the Web lurking to Scam Shoppers this Christmas: a Critical Analysis of the United Kingdom's Legislative Provisions and Policies to Tackle Online Fraud', *Information and Communications Technology Law,* 20(1) (2011), 35.
HARRINGTON, J., 'Extradition of Transnational Criminals'. *In:* BOISTER, N. & CURRIE, R. (eds.), *Routledge Handbook of Transnational Criminal Law,* (Routledge: 2014).
HARRIS, C., ROWBOTHAM, J. & STEVENSON, K., 'Truth, Law and Hate in the Virtual Marketplace of Ideas: Perspectives on the Regulation of Internet Content', *Information and Communications Technology Law,* 18(2) (2009), 155.
HAYASHI, M., 'The Information Revolution and the Rules of Jurisdiction in Public International Law'. *In:* DUNN, M., KRISHNA-HENSEL, S. & MAUER, V. (eds.), *The Resurgence of the State: Trends and Processes in Cyberspace Governance,* (Ashgate: 2007).
HENRICHS, W., 'Problems of Competence in International Law with Regard to the Punishment of Narcotic Drug Offences and the Extradition of Narcotics Offenders', *Bulletin on Narcotics*, (1960).
HEPPLE, B., 'Statutes: Race Relations Act 1965', *Modern Law Review,* 29(3) (1966), 306.
HERRNFELD, H.H., 'Mechanisms for Settling Conflicts of Jurisdiction'. *In:* LUCHTMAN, M. (ed.), *Choice of Forum in Cooperation Against EU Financial Crime,* (Eleven International Publishing: 2013).
HEWITT, M. & HOLMES, D., 'Overview of Problems Facing Police Investigation of Transnational Crime', *Investigating and Prosecuting*

Transnational Crime, (2002), proceedings of a One-Day Conference Organised by the Kent Criminal Justice Centre, University of Kent at Canterbury (10 July 2002).

HIRST, M., *Jurisdiction and the Ambit of the Criminal Law*, (Oxford Universisty Press: 2003).

HODGSON, T., 'The Gift that Keeps on Giving: Does the Protection Against Double Jeopardy have any Application to International Crime?', *Journal of Financial Crime,* 19(4) (2012), 326.

HOLT, T., 'Exploring the Social Organisation and Structure of Stolen Data Markets', *Global Crime,* 14(2) (2013), 155.

HOOPER, J. & ORMEROD, D. (eds.), *Blackstone's Criminal Practice*, (Oxford University Press: 2010).

HOSKINS, M, 'Briefing to the Joint Committee on the Draft Data Communications Bill', (2012), <http://www.parliament.uk/documents/joint-committees/communications-data/SPADpres0712.pdf>, (Accessed 20/12/2014).

HUFNAGEL, S., *Policing Cooperation Across Borders: Comparative Perspectives on Law Enforcement within the EU and Australia*, (Ashgate: 2013).

HUFNAGEL, S., HARFIELD, C. & BRONITT, S. (eds.), *Cross-Border Law Enforcement: Regional Law Enforcement Cooperation - European, Australian and Asia-Pacific Perspectives,* (Routledge: 2012).

HUFNAGEL, S. & MCCARTNEY, C., 'Police Cooperation Against Transnational Criminals'. *In:* BOISTER, N. & CURRIE, R. (eds.), *Routledge Handbook of Transnational Criminal Law,* (Routledge: 2014).

JACONELLI, J., 'Context-dependent Crime', *Criminal Law Review*, (1995), 771.

JOHNSON, D. & POST, D., 'Law and Borders: The Rise of Law in Cyberspace', *Stanford Law Review,* 48 (1996), 1367.

JOHNSON, J., 'The Long Arm of the Law'. *In:* LEGUM, B. (ed.), *International Litigation Strategies and Practice,* (American Bar Association: 2005).

JOUTSEN, M., 'International Instruments on Cooperation in Responding to Transnational Crime'. *In:* REICHEL, P. & ALBANESE, J. (eds.), *Handbook of Transnational Crime and Justice,* (Sage: 2014).

KAHLER, M. (ed.), *Networked Politics: Agency, Power, and Governance,* (Cornell University Press: 2009).

KAMMERHOFER, J., *Uncertainty in International Law: A Kelsenian Perspective*, (Routledge: 2011).

KASPERSEN, H., 'Jurisdiction in the Cybercrime Convention'. *In:* KOOPS, B.-J. & BRENNER, S. (eds.) *Cybercrime and Jurisdiction – A Global Survey,* (Springer: 2006).

KASPERSEN, H., 'Cybercrime and Jurisdiction', *Council of Europe Discussion Paper,* (2009), <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/2079_rep_Internet_Jurisdiction_rik1a%20_Mar09.pdf>, (Accessed 20/12/2014).

KELSEN, H., *General Theory of Law and State*, (Harvard University Press: 1946).

KELSEN, H., *Reine Rechtslehre,* 2nd ed., (Franz Deuticke, 1960).

KENT, G., 'Sharing Investigation-specific Data With Law Enforcement - An International Approach', (2014), <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2472413>, (Accessed 20/12/2014).
KEOHANE, R. & NYE, J., 'Transgovernmental Relations and International Organizations', *World Politics,* 27 (1974), 39.
KERR, O., 'Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes', *New York University Law Review,* 78 (2003), 1615.
KERR, O., 'Fourth Amendment Seizures of Computer Data', *Yale Law Journal,* 119 (2010), 700.
KERR, O., 'The Next Generation Communications Privacy Act', *University of Pennsylvania Law Review,* 162 (2014), 373.
KERRY, J., *The New War: The Web of Crime That Threatens America's Security,* (Touchstone: 1997).
KINGSBURY, B., KRISCH, N. & STEWART, R., 'The Emergence of Global Administrative Law', *Law and Contemporary Problems,* 68 (2005), 15.
KLIP, A., *European Criminal Law: An Integrative Approach*, (Intersentia: 2012).
KNOOK, A., 'The Court, the Charter, and the Vertical Division of Powers in the European Union', *Common Market Law Review,* 42 (2005), 367.
KOHL, U., *Jurisdiction and the Internet: Regulatory Competence over Online Activity*, (Cambridge University Press: 2007).
KOHL, U., 'Barbarians in Our Midst: 'Cultural Diversity' on the Transnational Internet', *European Journal of Law and Technology,* 5 (2014), 1.
KOOPS, B.-J. & BRENNER, S. (eds.), *Cybercrime and Jurisdiction – A Global Survey,* (Springer: 2006).
KOREMENOS, B., 'The Continent of International Law', *Journal of Conflict Resolution,* 57(4) (2013), 653.
KRAMER, L., 'Vestiges of Beale: Extraterritorial Application of American Law', *Supreme Court Law Review*, (1991) 179.
KRES, C., 'Universal Jurisdiction over International Crimes and the Institut de Droit International', *Journal of International Criminal Justice* 4(3) (2006), 561.
KROLIKOWSKI, M. & CLAES, E., 'The Limits of Legality in the Criminal Law'. *In:* CLAES, E., DEVROE, W. & KEIRSBILCK, B. (eds.), *Facing the Limits of the Law,* (Springer: 2009).
KYDD, A., 'Reputation and Cooperation: Guzman on international law', *International Theory,* 1(2) (2009), 295.
LEGUM, B. (ed.), *International Litigation Strategies and Practice,* (American Bar Association: 2005).
LEIDENMÜHLER, F., 'The Incorporation of the Schengen *acquis* into the Framework of the EU by Example of the "Ne Bis in Idem" Principle', *The European Legal Forum* 5 (2002), 253.
LESLIE, D. A., *Legal Principles for Combatting Cyberlaundering*, (Springer: 2014).
LESSIG, L., *Code: And Other Laws of Cyberspace*, (Basic Books: 1999).
LOMBOIS, C., *Droit Penal International*, (Dalloz: 1979).

LOWE, A., 'Blocking Extraterritorial Jurisdiction: The British Protection of Trading Interests Act, 1980', *The American Journal of International law,* 75(2) (1981), 257.
LOWE, V., 'The Principle of Non-intervention: Use of Force'. *In:* LOWE, V. & WARBRICK, C. (eds.), *The United Nations and the Principles of International Law: Essays in Memory of Michael Akehurst,* (Routledge: 1994).
LOWE, V. & WARBRICK, C. (eds.), *The United Nations and the Principles of International Law: Essays in Memory of Michael Akehurst,* (Routledge: 1994).
LOWENFELD, A., 'Public Law in the International Arena: Conflict of Laws, International Law, and Some Suggestions for their Interaction', *Recueil Des Cours,* 163 (1979), 311.
LOWES, P., *The Genesis of International Narcotics Control*, (Librairie Droz: 1966).
LUBAN, D., 'Fairness to Rightness: Jurisdiction, Legality, and the Legitimacy of International Criminal Law'. *In:* BESSON, S. & TASIOULAS, J. (eds.), *The Philosophy of International Law* (Oxford University Press: 2010).
LUCHTMAN, M., 'Principles of European Criminal Law: Jurisdiction, Choice of Forum, and the Legality Principle in the Area of Freedom, Security, and Justice', *European Review of Private Law,* 20(2) (2012), 347.
LUCHTMAN, M., (ed.), *Choice of Forum in Cooperation Against EU Financial Crime,* (Eleven International Publishing: 2013).
MACADO, S. (ed.), *Universal Jurisdiction: National Courts and the Prosecution of Serious Crimes under International Law*, (University of Pennsylvania Press: 2006).
MACEWAN, N., 'A Tricky Situation: Deception in Cyberspace', *Journal of Criminal Law,* 77(5) (2013), 413.
MAGNUSON, W., 'The Domestic Politics of International Extradition', *Virginia Journal of International Law,* 52 (2012), 839.
MANN, F.A., 'The Doctrine of Jurisdiction in International Law', *Recueil Des Cours,* 111 (1964), 1.
MANN, F.A., *Studies in International Law*, (Oxford Univsersity Press: 1973).
MANN, F.A., 'The Doctrine of International Jurisdiction Revisited After Twenty Years'. *In:* REISMAN, M. (ed.), *Jurisdiction in International Law,* (Ashgate: 1984).
MARION, N., 'The Council of Europe's Cyber Crime Treaty: An Exercise in Symbolic Legislation', *International Journal of Cyber Criminology,* 4(1) (2010), 699.
MARTHA, R., *The Legal Foundations of Interpol* (Hart Publishing: 2010).
MAY, L., *Crimes Against Humanity: A Normative Account*, (Cambridge University Press: 2005).
MCGUIRE, M. & DOWLING, S., 'Cyber Crime: A Review of the Evidence', (2013), Home Office, Research Report 75.
MCLUHAN, M., *The Gutenberg Galaxy: The Making of Typographic Man*, (University of Toronto Press: 1962).
MCNAIR, L., *International Law Opinions (selected and annotated by Lord McNair)*, (Cambridge University Press: 1956).
MEYER, J., 'The Vicarious Administration of Justice: An Overlooked Basis of Jurisdiction', *Harvard International Law Journal,* 31 (1990), 108.

MITCHELL, C., *Aut Dedere, aut Judicare: The Extradite or Prosecute Clause in International Law*, (The Graduate Institute of International and Development Studies: 2009), <http://books.openedition.org/iheid/249>, (Accessed 20/12/2014).
MITSILEGAS, V., *EU Criminal Law*, (Hart Publishing: 2009).
MOORE, J. B., 'Report on Extraterritorial Crime and the Cutting Case', (1887), <https://archive.org/details/reportonextrate00moorgoog> (Accessed 20/12/2014).
MOORE, J. B., *A Treatise on Extradition and Interstate Rendition: Volume I*, (The Boston Book Company: 1891).
MUELLER, M., *Network and States: The Global Politics of Internet Governance,* (MIT Press: 2010).
MURRAY, A., 'Volume Litigation: More Harmful than Helpful?', *Computers and Law,* 20(6) (2009), 43.
MURRAY, A., *Information Technology Law*, (Oxford University Press: 2013).
NADELMANN, E., 'Global Prohibition Regimes: The Evolution of Norms in International Society', *International Organization,* 44(4) (1990), 479.
NADELMANN, E., *Cops Across Borders: The Internationalization of US Criminal Law Enforcement,* (The Pennsylvania State University Press: 1993).
NATARAJAN, M. (ed.), *International Crime and Justice*, (Cambridge University Press: 2011).
NEAGU, N., 'The *Ne Bis in Idem* Principle in the Interpretation of European Courts: Towards Uniform Interpretation', *Leiden Journal of International Law,* 25(4) (2012), 955.
NEWMAN, A. & ZARING, D., 'Regulatory Networks: Power, Legitimacy, and Compliance'. *In:* DUNOFF, J. & POLLACK, M. (eds.), *Interdisciplinary Perspectives on International Law and International Relations,* (Cambridge University Press: 2013).
O'CONNOR, J., 'The Microsoft Warrant Case: Not Just an Irish Issue', *Computers and Law,* 25(4) (2014), 10.
O'FLOINN, M., 'Dealing with Domain Names used in Connection with Criminal Activity: Background Report on Views Expressed.' (2011). Nominet. <https://publicaffairs.linx.net/public/uk/Nominet/Report%20on%20Abuse%20Policy_M%20O%20Floinn_Final%20Web.pdf>, (Accessed 20/12/2014).
O'FLOINN, M., 'It Wasn't All White Light Before *Prism:* Law Enforcement Practices in Gathering Data Abroad, and Proposals for Further Transnational Access at the Council of Europe', *Computer Law and Security Review,* 29(5) (2013), 610.
O'FLOINN, M. & ORMEROD, D., 'Social Networking Sites, RIPA and Criminal Investigations', *Criminal Law Review,* 10 (2011), 766.
O'FLOINN, M. & ORMEROD, D., 'Social Networking Material as Criminal Evidence,' *Criminal Law Review,* 7 (2012), 486.
O'KEEFE, R., 'Universal jurisdiction: Clarifying the Basic Concept', *Journal of International Criminal Justice,* 2(3) (2004), 735.
O'KEEFE, R., 'Domestic Courts as Agents of Development of the International Law of Jurisdiction', *Leiden Journal of International Law* 26(3) (2013), 541.

OBOKATA, T., *Transnational Organised Crime in International Law*, (Hart Publishing: 2010).
OEHLER, D., *Internationales Strafrecht*, (Carl Heymanns Verlag: 1983).
OLSON, L., 'Re-enforcing Enforcement in a Specialised Convention on Crimes Against Humanity: Inter-state cooperation, Mutual Legal Assistance, and the Aut Dedere Aut Judicare Obligation'. *In:* SADAT, L. N. (ed.), *Forging a Convention for Crimes Against Humanity,* (Cambridge University Press: 2011).
OPPENHEIM, L., *International Law*, (Longmans, Green & Co: 1955).
ORMEROD, D., 'The Fraud Act 2006 - Criminalising Lying?', *Criminal Law Review*, (2007) 193.
ORMEROD, D., *Smith and Hogan's Criminal Law*, 13th ed., (Oxford University Press: 2011).
ORMEROD, D. & HUW-WILLIAMS, D., *Smith's Law of Theft*, (Oxford University Press: 2007).
PARRISH, A., 'The Effects Test: Extraterritoriality's Fifth Business', *Vanderbilt Law Review,* 61 (2008), 1455.
PARRISH, A., 'Domestic Responses to Transnational Crime: The Limits of National Law', *Criminal Law Forum,* 23(1) (2012), 275.
PARRISH, A., 'Evading Legislative Jurisdiction', *Notre Dame Law Review,* 87 (2012), 1673.
PASSAS, N., (ed.), *Transnational Crime*, (Dartmouth: 1999).
PEARSON, S. & YEE, G. (eds.), *Privacy and Security for Cloud Computing,* (Springer: 2013).
PECZENIK, A., 'Legal Research and Growth of Science', *Memoria del X Congreso Mundial Ordinario de Filosofía del Derecho y Filosofía Social,* (1981), < http://biblio.juridicas.unam.mx/libros/1/468/3.pdf> (Accessed 20/12/2014).
PEERS, S., 'Mutual Recognition and Criminal Law in the European Union: Has the Council got it Wrong?', *Common Market Law Review,* 41(1) (2004), 5.
PETERSON, N., 'How Rational is International Law?', *European Journal of International Law,* 20(4) (2009), 1247.
PICONE, P., 'The Distinction Between Jus Cogens and Obligations Erga Omnes'. *In:* CANNIZZARO, E. (ed.), *The Law of Treaties Beyond the Vienna Convention,* (Oxford University Press: 2011).
PINELLI, C., 'The Kelsen/Schmitt Controversy and the Evolving Relations between Constitutional and International Law', *Ratio Juris,* 23 (2010), 493.
PIRKER, B., 'Territorial Sovereignty and Integrity and the Challenges of Cyberspace'. *In:* ZIOLKOWSKI, K. (ed.), *Peacetime Regime For State Activities in Cyberspace: International Law, International Relations, and Diplomacy,* (NATO Cooperative Cyber Defence Centre of Excellence: 2013).
PLACHTA, M., '(Non-) Extradition of Nationals: A Neverending Story?', *Emory International Law Review,* 13 (1999), 77.
POST, D., 'Against "Against Cyberanarchy"', *17 Berkeley Technology Law Journal,* 17 (2002), 1363.
RAFARACI, T. & BELFIORE, R., 'Judicial Protection of Individuals under the Third Pillar of the European Union', *Jean Monnet Working Paper*,

(2007),<http://www.academia.edu/396285/Judicial_Protection_of_Individuals_under_the_Third_Pillar_of_the_European_Union>, (Accessed 20/12/2014).
RAM, C., 'The Globalization of Crime as a Jurisdictional Challenge', *The International Centre for Criminal Law Reform and Criminal Justice Policy* (2011).
RAM, C., 'Cybercrime'. *In:* BOISTER, N. & CURRIE, R. (eds.), *Routledge Handbook of Transnational Criminal Law*. (Routledge: 2014).
RAUSTIALA, K., 'The Architecture of International Cooperation: Transgovernmental Networks and the Future of International Law', *Virginia Journal of International Law,* 43(1) (2002), 1.
RAUSTIALA, K., 'Form and Substance in International Agreements', *American Journal of International Law,* 99 (2005), 581.
RAUSTIALA, K., 'The Geography of Justice', *Fordham Law Review,* 73(6) (2005), 2501.
RAUSTIALA, K., 'Empire and Extraterritoriality in Twentieth Century America', *Southwestern Law Review,* 40 (2011), 605.
REICHEL, P. & ALBANESE, J. (eds.), *Handbook of Transnational Crime and Justice,* (Sage: 2014).
REIDENBERG, J., 'Lex Informatica: The Formulation of Information Policy Rules through Technology', *Texas Law Review,* 76 (1997), 553.
REISMAN, M. (ed.), *Jurisdiction in International Law,* (Ashgate: 1984).
REYDAMS, L., *Universal Jurisdiction: International and Municipal Legal Perspectives*, (Oxford University Press: 2003).
RITCHIE, J., LEWIS, J., NICHOLLS, C.M. & ORMSTON, R. (eds.), *Qualitative Research Practice: A Guide for Social Science Students and Researchers*, (Sage: 2013).
ROBINSON, M., Preface. *In:* MACADO, S. (ed.), *Universal Jurisdiction: National Courts and the Prosecution of Serious Crimes under International Law,* (University of Pennsylvania Press: 2006).
ROSCINI, M., *Cyber Operations and the Use of Force in International Law*, (Oxford University Press: 2014).
ROZENSWEIG, P., 'The International Governance Framework for Cybersecurity', *Canada-United States Law Journal,* 37 (2012), 405.
RUGGERI, S. (ed.), *Transnational Inquiries and the Protection of Fundamental Rights in Criminal Proceedings,* (Springer: 2013).
RUMNEY, P., 'The British Experience of Racist Hate Speech Regulation: A Lesson for First Amendment Absolutists?', *Common Law World Review,* 32(2) (2003), 117.
RYNGAERT, C., *Jurisdiction in International Law*, (Oxford University Press: 2008).
RYNGAERT, C., 'Territorial Jurisdiction Over Cross-Frontier Offences: Revisiting a Classic Problem of International Criminal Law', *International Criminal Law Review,* 9 (2009), 187.
SADAT, L. N. (ed.) *Forging a Convention for Crimes Against Humanity,* (Cambridge University Press: 2011).
SANSOM, G., 'Strategies of Displacement and Other Violations of Territoriality: Cybercrime, the World Wide Web and the Ambit of Criminal Law'. *In:* BRETON, A. (ed.), *Multijuralism: Manifestations, Causes, and Consequences,* (Ashgate: 2009).

SASSEN, S., 'When Territory Deborders Territoriality', *Territory, Politics, Governance,* 1(1) (2013), 21.
SCASSA, T. & CURRIE, R., 'New First Principles? Assessing the Internet's Challenges to Jurisdiction', *Georgetown Journal of International Law,* 42 (2011), 1017.
SCHJOLBERG, S., 'The History of Global Harmonization on Cybercrime Legislation: The Road to Geneva', (2008), <http://www.cybercrimelaw.net/documents/cybercrime_history.pdf>, (Accessed 20/12/2014).
SCHJOLBERG, S., *The History of Cybercrime 1976-2014*, (Cybercrime Research Institute: 2014).
SCHMITT, M. (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, (Cambridge University Press: 2013).
SCHULTZ, T., 'Carving up the Internet: Jurisdiction, Legal Orders and the Private/Public International Law Interface', *European Journal of International Law,* 19 (2008), 799.
SCHWARZENBERGER, G., *The Dynamics of International Law*, (Professional Books: 1976).
SEITZ, N., 'Transborder Search: A New Perspective in Law Enforcement?', *Yale Journal of Law and Technology,* 7(1) (2005), 23.
SHACKELFORD, S., *Managing Cyber Attacks in International Law, Business, and Relations*, (Cambridge University Press: 2014).
SHELLEY, L., 'The Globalization of Crime'. *In:* NATARAJAN, M. (ed.), *International Crime and Justice,* (Cambridge University Press: 2011).
SHEPTYCKI, J. (ed.), *Issues in Transnational Policing*: (Routledge: 2000).
SIGLER, J., 'A History of Double Jeopardy', *American Journal of Legal History,* 7(4) (1963), 283.
SILVERMAN, D., *Doing Qualitative Research,* (Sage: 2005).
SLAUGHTER, A-M., *A New World Order*, (Princeton University Press: 2004).
SLIEDREGT, E.V., 'The European Arrest Warrant: Between Trust, Democracy and the Rule of Law', *European Constitutional Law Review,* 3 (2007), 244.
SOGHOIAN, C., 'Caught in the Cloud: Privacy, Encryption and Government Back Doors in the Web 2.0 Era', *Journal on Telecommunications and High Technology Law,* 8(2) (2010), 359.
SOMMER, P., 'Police Powers to Hack: Current UK Law', *Computer and Telecommunications Law Review,* 18(6) (2012), 165.
SOUKIEH, K., 'Cybercrime – The Shifting Doctrine of Jurisdiction', *Canberra Law Review,* 10 (2011), 221.
SPENCER, J., 'Mutual Recognition and Choice of Forum', *In:* LUCHTMAN, M. (ed.), *Choice of Forum in Cooperation Against EU Financial Crime,* (Eleven International Publishing: 2013).
STANBROOK, I. & STANBROOK, C., *Extradition Law and Practice*, (Oxford University Press: 2000).
STESSENS, G. & WYNGAERT, C.V.D., 'The International Non Bis in Idem Principle: Resolving Some of the Unanswered Questions', *International and Comparative Law Quarterly* (1990), 779.
STIMSON, E., *Conflict of Criminal Laws*, (Foundation Press: 1936).

SVANTESSON, D., 'Between a Rock and a Hard Place - An International Law Perspective of the Difficult Position of Globally Active Internet Intermediaries', *Computer Law and Security Review,* 30 (2014), 348.
SWIRE, P., 'Of Elephants, Mice, and Privacy: International Choice of Law and the Internet. *International Lawyer,* 32 (1998), 991.
TRUBEK, D., & TRUBEK, L., 'Hard and Soft Law in the Construction of Social Europe: the Role of the Open Method of Co-ordination' *European Law Journal* 11(3) (2005), 343.
TRUDEL, P., 'Jurisdiction Over the Internet: A Canadian Perspective', *International Lawyer,* 32 (1998), 1027.
URBAS, G., 'Cybercrime, Jurisdiction and Extradition: The Extended Reach of Cross-Border Law Enforcement', *Journal of Internet Law,* 16(1) (2012), 7.
VERDIER, P.H., 'Transnational Regulatory Networks and Their Limits', *Yale Journal of International Law,* 34 (2009), 113.
VERMEULEN, G., BONDT, W.D. & RYCKMAN, C., 'Rethinking International Cooperation in Criminal Matters in the EU', *IRCP Research Series,* 42 (2012).
VERVAELE, J., 'Mutual Legal Assistance in Criminal Matters to Control (transnational) Criminality'. *In:* BOISTER, N. & CURRIE, R. (eds.), *Routledge Handbook of Transnational Criminal Law,* (Routledge: 2014).
WALDEN, I., 'Harmonising Computer Crime Laws in Europe', *European Journal of Crime, Criminal Law and Criminal Justice,* 12(4) (2004), 321.
WALDEN, I., *Computer Crimes and Digital Investigations*, (Oxford University Press: 2007).
WALDEN, I., 'Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent'. *In:* PEARSON, S. & YEE, G. (eds.), *Privacy and Security for Cloud Computing,* (Springer: 2013).
WALKER, N. (ed.), *Sovereignty in Transition*, (Hart Publishing: 2003).
WALL, D., (a) 'Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace', *Police Practice and Research: An International Journal,* 8(2) (2007), 183.
WALL, D., (b) *Cybercrime: The Transformation of Crime in the Information Age*, (Polity Press: 2007).
WARREN, C. & KARNER, T., *Discovering Qualitative Methods*, (Roxbury: 2005).
WATSON, G., 'Offenders Abroad: The Case for Nationality-Based Criminal Jurisdiction', *Yale Journal of International Law,* 17 (1992), 41.
WEBER, M., 'Politics as a Vocation'. *In:* GERTH, H.H. & MILLS, C.W. (eds.), *From Max Weber: Essays in sociology,* (Routledge: 1948).
WEDGWOOD, R., 'The Revolutionary Martyrdom of Jonathan Robbins', *The Yale Law Journal* 100 (2009), 229.
WEILER, J. & LOCKHART, N., 'Taking Rights Seriously Seriously: The European Court and its Fundamental Rights Jurisprudence - Part 1', *Common Market Law Review,* 32(1) (1995), 51.
WHEATON, H., *Elements of International Law*, (Brown and Co: 1866).
WHITTY, M. & BUCHANAN, T., 'The Psychology of the Online Dating Romance Scam', (2012), <http://www2.le.ac.uk/departments/media/people/monica-whitty/Whitty_romance_scam_report.pdf>, (Accessed 20/12/2014).

WIJNGAERT, C.V.D.. *The Political Offence Exception to Extradition: The Delicate Problem of Balancing the Rights of the Individual and the International Public Order*, (Kluwer Law International: 1980).

WILLIAMS, G., 'Venue and the Ambit of Criminal Law - Part 1', *Law Quarterly Review,* 81 (1965), 276

WILLIAMS, G., 'Venue and the Ambit of Criminal Law - Part 2', *Law Quarterly Review,* 81 (1965), 395.

WILLIAMS, G., 'Venue and the Ambit of Criminal Law - Part 3', *Law Quarterly Review,* 81 (1965), 518.

WILLIAMS, P., 'Transnational Criminal Organisations and International Security'. *In:* PASSAS, N. (ed.), *Transnational Crime,* (Dartmouth: 1999).

WILLIAMS, S., 'Nationality, Double Jeopardy, Prescription and the Death Sentence As Bases for Refusing Extradition', *International Review of Penal Law,* 62 (1991), 259.

WOOD, M. & JAMNEJAD, M., 'The Principle of Non-Intervention', *Leiden Journal of International Law* 22 (2009), 345.

YOUNG, P., 'Current Issues: Extradition', *Australian Law Journal* 81 (2007), 223.

ZIOLKOWSKI, K. (ed.), *Peacetime Regime For State Activities in Cyberspace: International Law, International Relations, and Diplomacy,* (NATO Cooperative Cyber Defence Centre of Excellence: 2013).

ZIOLKOWSKI, K., 'General Principles of International Law as Applicable in Cyberspace'. *In:* ZIOLKOWSKI, K. (ed.), *Peacetime Regime For State Activities in Cyberspace: International Law, International Relations, and Diplomacy,* (NATO Cooperative Cyber Defence Centre of Excellence: 2013).