CYBERCRIME – THE SHIFTING DOCTRINE OF JURISDICTION

KIM SOUKIEH*

I INTRODUCTION

The legal requirement of jurisdiction can create a number of practical challenges in the investigation and prosecution of 'offline' crimes.[1] Perpetrators are able to move between state borders, often exploiting nuances in the law to their advantage and making apprehension a complex and costly undertaking. In the 'online' world this complexity and expense is substantially increased as state and national boundaries give way to trans-global communications passing through vastly different political and legal systems, often with radically different notions of criminality.[2] Even where there is a large degree of conformity in national laws and cooperation between governments, courts around the world run into problems in asserting jurisdiction. (See the examples of the Russian extortionists,[3] the Lithuanian fraudsters,[4] and the Filipino

* Student editor, Faculty of Law, University of Canberra.

[1] The author uses the terms 'online' and 'offline' to make a broad distinction between computer and non-computer related offences.

[2] Susan Brenner & Bert-Jaap Koops, 'Approaches to Cybercrime Jurisdiction' (2003) 4(1) *Journal of High Technology Law*, 3.

[3] P Atfield, *United States v Gorshkov Detailed Forensics and Case Study: Expert Witness Perspective* (2011) IEEE Explore <http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?reload=true&arnumber=1592518>; *United States v.Gorshkov*, (Case No:CR00-550C, US District Court for the Western District of Washington, 2001).

[4] See: Agence France-Presse, 'Lithuania Refuses Extradition to US for Cyber-crime Suspect', *The Brisbane Times* (online), 25 July 2007, <http://news.brisbanetimes.com.au/technology/lithuania-refuses-extradition-to-us-for-cybercrime-suspect-20070725-pki.html>.

men behind the 'love bug' virus,[5] below). The difficulty in answering the question, 'who has jurisdiction', in any given scenario, arguably, reflects the difficulty in attempts to harmonise cybercrime laws internationally. What is perfectly legal in one jurisdiction may amount to a serious offence in another so that, as Brenner observed, when an adult entertainment business operating successfully for three years in Germany decides to conduct its business over the internet, 'it finds itself confronted with the criminal laws of all countries connected to the Internet, that is, all countries of the world'.[6] In that instance, serious charges were laid against the company and its operators in both Belgium and Singapore.[7]

The aim of this paper is to explore those aspects of jurisdiction which pose difficulties for cybercrime law enforcement, and examine the ways in which law makers have responded, both in Australia and internationally. This discussion focuses on issues related to extraterritorial claims over cybercrimes. For example, the laws of virtually all modern democracies posit 'territoriality' as the basis for acquiring criminal jurisdiction,[8] yet the criminal conduct in cybercrimes may originate from a number of geographical locations, and its impact may have been global.[9] Who then has jurisdiction to prosecute? Related issues include situations where elements of an offence take place in more than one jurisdiction and access from one jurisdiction to

[5] Brenner & Koops above n 2, 6-7.
[6] Atfield above n 3.
[7] Brenner & Koops above n 2, 3.
[8] Ibid, 10.
[9] Larry Seltzer, 'I Love You Turns 10, What Have We Learned?', *PC Magazine* (online), April 2010, <http://www.pcmag.com/article2/0,2817,2363172,00.asp>.

digital evidence in another jurisdiction has the potential to raise concerns about privacy, security and national sovereignty.[10]

Additionally, there is no guarantee that national laws, no matter how well conceived, will be effective where offenders reside elsewhere. 'Enforcement' remains the most difficult aspect of jurisdiction.[11] This may be so even where there are good bilateral relations and extradition provisions in place. For example, how does a country request the extradition of an alleged offender if the requested nation has no equivalent offence?[12] What if there are wide discrepancies in the types of punishment and sentencing?[13] Another issue faced by law makers is a tendency towards the politicisation of the extradition process, so that, whether or not an extradition treaty exists, the process may elicit unpredictable responses.[14] This brings the discussion to the central contention of this paper, which is the absolute necessity of a comprehensive international cybercrime treaty. Jurisdictional 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.[15]

---

[10] Atfield, above n 2.
[11] Jonathon Clough, *Principles of Cybercrime* (Cambridge, 2010) 413.
[12] This relates to the international law notion of 'double criminality' which is explored on page 5 of the article.
[13] Chapter 7 of: R G Smith, *Judicial Punishment in Cyberspace, Cyber Criminals on Trial*, (Cambridge University Press, 2004) 106-123.
[14] See generally: above n 4; John Leydon, *Russians Accuse FBI Agent of Hacking* (19 August 2002) The Register <http://www.securityfocus.com/news/584>.
[15] See: National Interest Analysis White Paper titled: *Accession by Australia to the Convention on Cybercrime* (2011) <http://www.securitymanagement.com.au/content/file/Convention_analysis.pdf>.

It should be noted that 'cybercrime' is still a relatively new concept to contemporary criminal and international law, and many highly publicised controversies never actually reach the courts, precisely because of a lack of jurisdiction. This is particularly evident in lack of 'double criminality' cases,[16] but can also be a consequence of any number of laws peculiar to a nation, and which prevent cybercrimes ever being adjudicated or brought before a court.[17] Therefore, many of the examples used in this paper to illustrate jurisdictional issues are gleaned, not only from legislation and case law, but from news reports, specialist websites and other widely recognised resources.

II PRELIMINARY MATTERS

In relation to the term 'cybercrime', this paper follows the widely accepted three-stage classification set out by Jonathan Clough,[18] which itself mirrors the US Department of Justice definition.[19] Cybercrimes are crimes in which a computerised device or network is the target of criminal activity; crimes where the computer is used to commit a recognised offence; and crimes in which the computer is incidental to the commission of a crime.[20]

---

[16] See, Clough above n 11, 405-416
[17] See generally: Stein Schloberg, *A Global Treaty on Cybersecurity and Cybercrime* (2011) <http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf>.
[18] Clough, above n 11, p 10.
[19] *National Information Infrastructure Protection Act 1996* (US), s 1030.
[20] Clough Above n 11, p 10.

Criminal law jurisdiction involves three issues - prescription, adjudication and enforcement:

- Jurisdiction to prescribe is a sovereign entity's authority to make its law applicable to the activities, relations, or status of persons, or the interests of persons in things by legislation, by executive act or order, by administrative rule, or by determination of a court.
- Jurisdiction to adjudicate is a sovereign entity's authority to subject persons or entities to the process of its courts or administrative tribunals for the purpose of determining whether prescriptive law has been violated.
- Jurisdiction to enforce is a sovereign entity's authority to induce or compel compliance or to punish non-compliance with its laws or regulations.[21]

In the context of cybercrimes, this categorisation is not simply of theoretical interest, but underscores the component steps that legislators and courts must consider before commencing prosecutions, nationally and extraterritorially.[22] The greatest area of difficulty, and controversy, relates to the enforcement aspect of jurisdiction, especially with regard to the 'territorial' nature of criminal jurisdiction.[23]

[21] Brenner & Koops above n 2, 5.
[22] Clough above n 11, 406-416.
[23] Ibid, 413.

III JURISDICTION – INITIAL CONSIDERATIONS

Often, the first stumbling block for law enforcement in the prosecution of cybercrime offenders will be the question of which feature of the conduct is a precondition for acquiring jurisdiction. Is it the location where the conduct was initiated, the nationality of the offender, or the location where the effect was felt? Brenner and Koopps' comparative study of jurisdiction clauses in legislation from around the world found that much of the law in this area remains stubbornly traditional, so that despite the non-physical nature of the internet, 'territoriality' is still a prime factor.[24] In particular, the place where the illegal conduct is initiated remains the central ingredient for acquiring jurisdiction. That is not to say laws are uniform; some countries consider both the place of the act and its effect as having equal weight,[25] while others are satisfied as long as there is any causal jurisdictional nexus to the crime.[26] Despite this, there is overwhelming evidence that the physical location where the act took place remains paramount, and that this is too limited a perspective in light of the geographical sweep of most cybercrimes.[27] Brenner observes:

> The interpretation of particularly the location of the act will create problems in cybercrime, where the origins and destinations of the crime are usually in different locations, and where the means, computer networks and IP packets, usually cross numerous territories.[28]

Perhaps jurisdiction should be based on the location where the offending conduct had its effect? What about nationality? Should there also be a consideration of the

---

[24] Brenner above n 2, 44.
[25] See, eg, *Criminal Code Act 1995* (Cth), s 15(1)(a) and 15(1)(b).
[26] Brenner above n 2, 13, quoting: *West Virginia Computer Crimes and Abuse Act.*
[27] Ibid 44-46.

originating State where the offending technology was created, along with any intermediary State facilitators? Australia's Commonwealth legislation has gone some way to addressing these issues. For example, while ss 477 and 478 of the *Criminal Code Act 1995* (Cth) set out the most common bases for criminal jurisdiction, s 15.1(1)(b) specifically addresses situations where the criminal conduct takes place elsewhere but 'wholly or partly' affects Australia. Additionally, 'citizenship' is included as a basis for extended jurisdiction under paragraph 15.1(1)(c). These provisions collectively broaden the reach of Australian cybercrime enforcement.

Significantly, the *European Convention on Cybercrime*, which is discussed in more detail below, has addressed these issues firstly through Articles 2 to 11, which set out a cybercrime typology,[29] and then through Article 22(1)(a) which establishes the territorial basis for acquiring jurisdiction and includes 'effect' and 'citizenship' as a basis for jurisdiction. These approaches, if adopted by major countries, have the potential to address the trans-nationality of cybercrime.

Cybercrimes can also create difficulties where some essential element of the offence has taken place outside the prosecuting territory. This question came before the courts in Australia relatively early in two seminal cases. In *DPP v Sutcliffe*,[30] a cyber-stalking case, the problem before the courts was that the victim was at all times living in Canada, so that one of the essential elements of the offence, that of instilling fear in the victim, took place outside Victoria. The Melbourne Magistrates' Court found that

---

[28] Ibid, 44.
[29] ie a recognition and codification of various types of cybercrimes
[30] *DPP v Sutcliffe* (2001) VSC 43.

stalking had not been made out and the case was dismissed.[31]On appeal the Victorian Supreme Court held that the relevant state legislation did have extra-territorial effect, and that as long as a 'substantial' part of the offence was committed in Victoria, the defendant could be dealt with in Victoria, even though the victim was located in Canada.[32]

Gillard J stated:

> It follows in my opinion that the Magistrate was wrong in dismissing the charge of stalking against the respondent on the ground that the Magistrates' Court lacked jurisdiction. In my opinion it does have jurisdiction to hear the charge against the respondent even though the essential ingredient of the offence, namely proof of the harmful effect, will involve proving the effect of the alleged stalking on a person who at all relevant times was resident in Canada.[33]

The case triggered a flurry of legislation in Victoria with s 21A(7) of the *Crimes* Act *1958* (Vic) putting the issue beyond doubt. [34]

Similarly, in *Gutnick v Dow Jones & Co Inc*,[35] the Court had to decide whether it had jurisdiction over a US internet publisher Dow Jones, which it was alleged had defamed Mr Gutnick. Dow Jones argued that the Victorian courts did not have jurisdiction to hear the case because the defamation took place in New Jersey at the moment the offending story was uploaded onto servers there. Hedigan J held that

---

[31] *Sutcliffe v DPP* 07/04/03. Reference: Q1/2003
[32] *DPP v Sutcliffe*, above n 31, ¶45.
[33] Ibid, ¶103.
[34] Clough above n 11, 410
[35] *Gutnick v Dow Jones & Co Inc* [2001] VSC 305 (Unreported).

publication of material via the internet occurred where it was downloaded and read, not where it was uploaded onto a server.[36] Therefore Mr Gutnick's cause of action arose in Victoria. This finding was upheld by the High Court.[37]

IV JURISDICTION AND EXTRADITION

With respect to jurisdiction in the context of extraterritorial claims over cybercrimes, there are routinely two types of controversies that arise. Firstly, there are those occasions where a number of states are vying for jurisdiction (positive jurisdiction conflicts), and secondly, there are those where there is an expectation that another state will claim jurisdiction, but it fails to do so (negative jurisdiction conflicts).[38] The 'love bug' virus is often used as an example of the former, but in fact provides an example of both. After damages estimated at over US$10 billion, and law enforcement agencies worldwide clamouring for their extradition, Lamores and de Guzman (who were the creators and disseminators of the virus, and who had already confessed) were released, with all charges dropped by Philippine state prosecutors. The simple fact was that, at that time, virus dissemination was not a crime in the Philippines.[39]

---

[36] Ibid, Hedigan J, ¶60.
[37] *Dow Jones & Co Inc v Gutnick* [2002] HCA 56.
[38] Brenner above n 2, 40-41.
[39] Arnold Wayne, 'Technology: Philippines to Drop Charges on E-Mail Virus', *The New York Times* (New York), 22 August 2000.

The 'love bug' episode also provides an interesting example of the international law concept of 'double criminality'. This is the requirement that a person may only be extradited where the crime is recognised in both countries, usually subject to a minimum jail term of 12 months.[40] Because the Filipino men had committed no crime in their own country, the requirement of double criminality had not been met, and the US was refused extradition.[41] Double criminality can also provide a prime example of the tension between one country's desire to enforce its laws and another country's determination to preserve its legal sovereignty.[42] Yet the rationale underpinning the rule, and the reason for its continued resilience in international law, is to prevent criminals from evading justice by simply removing themselves from a geographical location. It should be noted that a refusal to extradite on the basis of double criminality may also serve a humanitarian role as a last defence for persons suffering religious or political persecution, or arbitrary punishment.

V THE NEED FOR AN INTERNATIONAL CONSENSUS

It should be noted that in the absence of extradition, or any other agreement, the potential for unforseen outcomes can be startling. It is worth mentioning here the controversial case of Vasiliy Gorshkov, who was sentenced to thirty-six months in a US prison after being convicted on 20 counts of conspiracy, various computer crimes,

[40] Clough, above n 11, 414.
[41] Arnold above n 38.
[42] Meaning that 'double criminality' can also act as a shield, preserving the States' legal autonomy.

and fraud committed against the Speakeasy Network of Seattle, Washington.[43] Gorshkov had been lured from Russia to the US by FBI agents posing as potential employers, and then arrested. There being no extradition treaty between the two countries, and limited cooperation between law enforcement agencies, the FBI sourced their information about Gorshkov by hacking a pair of computers in Russia. In an unprecedented response the Russian Federal Security Service charged the agent (Michael Schuller) with 'unauthorised accesses'.[44] Whatever the merits of these charges, the whole incident shows how, in the absence of any international consensus, enforcement activities can be misconstrued as either an attack on national sovereignty, or, as in the example below, be open to politicisation.

Even where there is close cooperation, an independent judiciary will prefer its own interpretation of its nation's obligations, even though there may be compelling reasons to do otherwise. This was true in the case of the Lithuanian, Paulius Kalpokas, who was arrested and charged after a joint US-Lithuanian sting operation caught him allegedly defrauding a number of US online stores.[45] There was a high expectation that co-operation would extend to the extradition of Kalpokas to the US where charges had already been laid against him. Instead, the appeals court decided that after hearing all arguments, Lithuania's legislation did not provide grounds for extraditing Kalpokas to the US.[46] According to reports, the appeals court held that other

---

[43] *United States v Gorshkov*, (Case No:CR00-550C), US District Court for the Western District of Washington, 2001).
[44] Leydon, above n 14.
[45] Sydney Morning Herald, 'Lithuania Refuses Extradition to US for Cybercrime' Sydney Morning Herald (online) 25 July 2007 <http://www.smh.com.au/news/Technology/Lithuania-refuses-extradition-to-US-for-cybercrime-suspect/2007/07/25/1185043133392.html>.
[46] Ibid.

international law covenants took precedence, so that as a European member state, Lithuanians should be afforded the benefits of the *European Convention on Human Rights*, including freedom from excessively long legal probes.[47]

VI INTERNATIONAL DEVELOPMENTS

Initially, the *Council of Europe Convention on Cybercrime* (Cybercrime Convention), which specifically addressed many of these issues, seemed to offer a way forward. Created in 2001, it came into force in 2004, and by 2010 had 46 signatories, including the US.[48] A comprehensive international consensus seemed a very realistic prospect. But in the seven years since its inception a number of issues remain outstanding. Only 30 of the 46 signatories have actually ratified the treaty, and there are still some major players unwilling to participate. At the time of writing, Russia, China, India and the Koreas continue to abstain from acceding to the Cybercrime Convention.[49] Also at the time of writing, Australia was only a signatory to the treaty and despite urgings from the international community,[50] has yet to accede to the convention.[51]

---

[47] Ibid.
[48] See Figure 1. Also:*Cybercrime: A Threat to Democracy, Human Rights and the Rule of Law* (2011) Council of Europe <http://www.coe.int/t/dc/files/themes/cybercrime/default_EN.asp>.
[49] See Table 1.
[50] Nigel Phair, 'Cybercrime and the Legal Dimension' (Speech delivered at the AusCERT Asia Pacific Information Security Conference 2009, Gold Coast 19-05-2009), 118 <http://www.aph.gov.au/house/committee/coms/cybercrime/report/chapter6.pdf>.
[51] *Proposed Accession to the Council of Europe Convention on Cybercrime* (2011) Attorney-General's Department, <http://www.ema.gov.au/www/agd/agd.nsf/Page/Consultationsreformsandreviews_ProposedAccessiontotheCouncilofEuropeConventiononCybercrime>.

Another reason that has been cited for the Cybercrime Convention's 'middling' success is that it lacks any recognition of the role of non-government entities,[52] and, as has been argued elsewhere, effective policing must at the very least include business and the online security community to be effective.[53] While the Cybercrime Convention remains the most comprehensive attempt to address many of these issues, it remains to be seen whether it can regain its former momentum. As it is, many sections remain insubstantial or non-committal. For example on 'positive jurisdiction' claims Article 22(5) provides:

> When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Despite this there are many other aspects of the Cybercrime Convention that should be considered a success. There have also been recent moves to extend its membership at a more accelerated rate,[54] but it remains to be seen whether this will be successful. Also worth mentioning here is the International Telecommunications Union, which has been making steady progress with its International Multilateral Partnership Against Cyber Threats (IMPACT), and interestingly, has made the inclusion of technologically developing nations a priority.[55] A recent Memorandum of Understanding signed between ITU and the United Nations Office on Drugs and

---

[52] Gady Franz-Stefan, *Towards a New Harmonized Global Framework on Cybercrime* (04 March 2011) East-West Institute <http://www.ewi.info/time-right-cyberspace-treaty>.
[53] See generally: *Strategies for Cybersecurity and Critical Information Infrastructure Protection* (2011) International Telecommunications Union <http://www.itu.int/ITU-D/cyb/cybersecurity/strategies.html>.
[54] See generally: The Cybercrime Convention Committee, *Modalities of Accession by Third Countries to the Convention on Cybercrime* (2010) Council of Europe <http://www.coe.int/t/dghl/standardsetting/t-cy/T-CY%20June%202010%20documents%20E+F/T-CY%20%282010%29%2006%20E.pdf>.

Crime (UNODC) on 19 May at the 2011 WSIS Forum event in Geneva, will see the two organisations collaborate in assisting ITU and UN Member States mitigate the risks posed by cybercrime.[56] Despite all this, the Cybercrime Convention remains the only internationally binding agreement whose articles comprehensively address jurisdictional issues. A more comprehensive agreement has not been forthcoming, and a Russian proposal for a global cybercrime treaty was rejected by the United Nations as recently as April 2010.[57]

Yet, if we are to believe news reports, cybercrime is now costing the global economy in excess of one trillion (US) dollars annually.[58] It is submitted that the international community remains divided as to the degree of cooperation they are willing to provide for effective cybercrime law enforcement. It is also generally recognised that it is still the online technical, business and social community that is the front line when it comes to deflecting imminent threats to communications infrastructure and the World Wide Web.[59] But it is still crucial that there are real legal consequences for cybercrime offenders and that the international community remains engaged on the issue. It is further submitted that while jurisdictional issues are but a subset of broader considerations within criminal and international law, they represent, potentially, the most enduring obstacles to effective cybercrime policing globally.

---

[55] Ibid.
[56] International Telecommunications Union, 'ITU Announces Significant New Landmarks in the Fight against Cyberthreats' (Press Release, 2011) <http://www.itu.int/net/pressoffice/press_releases/2011/17.aspx> 57; 12th UN Congress on Crime Prevention and Criminal Justice, <http://www.un.org/News/Press/docs/2010/soccp349.doc.htm>.
[58] David DeWalt, *Unsecured Economies – A Trillion Dollar Headwind* (2009) McAfee <http://blogs.mcafee.com/corporate/ceo-perspectives/unsecured-economies-%E2%80%93-a-trillion-dollar-headwind>.

VII CONCLUSION

Interdependent communications systems supporting trade, banking and other crucial infrastructure now take place on such a scale they position 'cybercrime' at a critical juncture between national law enforcement and international security.[60] Increasingly, solutions to jurisdictional issues, (and by extension cybercrime law enforcement), are inextricably linked to the future prosperity and stability of the international community and the global economy.

The advent of cybercrime has placed pressure on former concepts of jurisdiction in both criminal and international law. 'Territoriality' can no longer serve as the central basis for jurisdictional claims, and extraterritorial claims will have to be met through the development of binding bilateral and/or multilateral agreements. An inescapable conclusion of this paper is that jurisdictional issues will continue to persist until a comprehensive international consensus is reached. Cybercrime policing, in particular, is only as effective as its weakest link, and while nations refrain from participating in treaty making and collective law enforcement, the prosecution of offenders, hiding behind so-called safe-harbour provisions, will continue to prove difficult.[61] As things

---

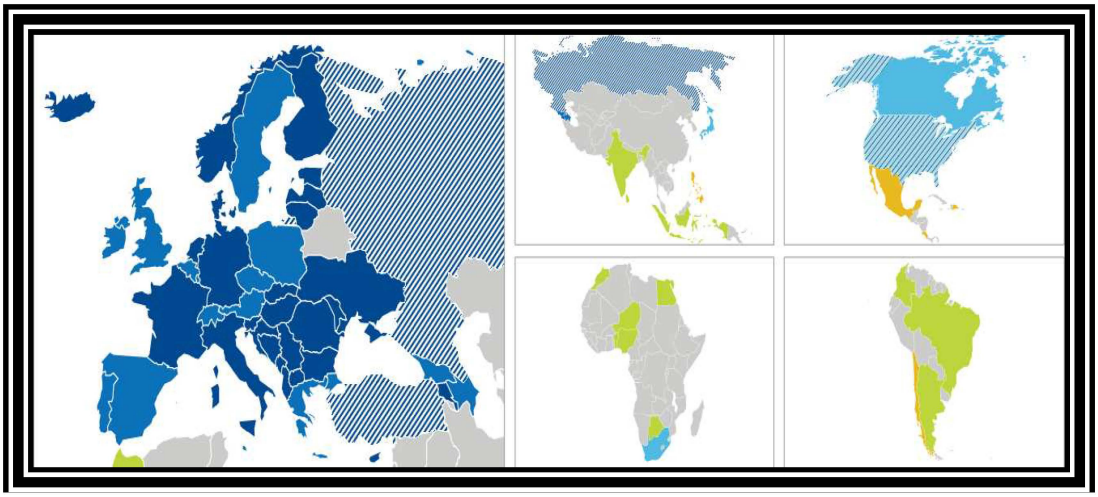
[59] M.L. Mueller, Chapter 8, 'Security Governance on the Internet', in: *Networks and States: the Global Politics of Internet Governance* (MIT Press, 2010) 162.
[60] See generally*: The Fourth Regional Conference on Cybercrime and International Criminal Co-operation (CICC) 2011, Security and Law in the Information* (2011) <http://www.inspiringwomen.org.au/LinkClick.aspx?fileticket=vGYVT8ctOMQ%3D&tabid=290>.
[61] Martha Arias, *Parody: A Safe Harbour under the Anti-Cybersquatting Protection Act* (2010) International Business Law Services <http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=2147>.

stand, even a cohesive cybercrime typology is proving difficult. But this is not to say that international treaty attempts have been pointless. There is no doubt that despite the recent inertia of the Cybercrime Convention, it remains the only comprehensive attempt to date to systematically set out the shared rights and obligations of members States, and which directly address the question of jurisdiction. But, as with any treaty, convention, or other legally binding multilateral instrument, it would be naïve to ignore the inevitable clash between the international community's desire for harmony and the nation State's desire for self-determination and legal autonomy. Issues over jurisdiction in cybercrime exemplify, and often amplify, this tension. Jurisdiction to access and retrieve information also falls into this category, and while some treaties explicitly recognise this,[62] where it is lacking there is always the temptation to act unilaterally, which only exacerbates political tension, as was the case in *United States v. Gorshkov* mentioned above. Even five years ago one might have been labelled alarmist in labouring these points too much, but the phenomenal integration that has taken place between modern communications technologies and almost every aspect of contemporary life, now puts cybercrime law enforcement at the forefront of international community concerns.

[62] *Council of Europe Convention on Cybercrime*, Article 25.

VIII APPENDICES

A Appendix I: Distribution of Cyber Convention Signatories



Countries party to the Convention

Council of Europe member states

Albania, Armenia, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Latvia, Lithuania, Moldova, Montenegro, Netherlands, Norway, Romania, Serbia, Slovak Republic, Slovenia, «the former Yugoslav Republic of Macedonia », Ukraine

Non Council of Europe member states

United States*

Signatory countries

Council of Europe member states

Austria, Azerbaijan, Belgium, Czech Republic, Georgia, Greece, Ireland, Liechtenstein, Luxembourg, Malta, Poland, Portugal, Spain, Sweden, Switzerland, United Kingdom

Non Council of Europe member states

South Africa, Canada*, Japan*

Countries which did neither ratify nor sign the Convention

Council of Europe member states

Andorra, Monaco, Russia, San Marino, Turkey

Countries that are known to use the Convention as a guideline for their national legislation

Non Council of Europe member states

Argentina, Botswana, Brazil, Colombia, Egypt, India, Indonesia, Morocco, Nigeria, Sri Lanka

Non Council of Europe member states invited to accede

Chile, Costa Rica, Dominican Republic, Mexico*, Philippines

* observer countries

B Appendix II: Status of Member Nations

States	Signature	Ratification	Entry into force	Notes	R.	D.	A.	T.	C.	O.
Albania	23/11/2001	20/6/2002	1/7/2004				X			
Andorra										
Armenia	23/11/2001	12/10/2006	1/2/2007				X			
Austria	23/11/2001									
Azerbaijan	30/6/2008	15/3/2010	1/7/2010		X	X	X	X		
Belgium	23/11/2001									
Bosnia and Herzegovina	9/2/2005	19/5/2006	1/9/2006				X			
Bulgaria	23/11/2001	7/4/2005	1/8/2005		X	X	X			
Croatia	23/11/2001	17/10/2002	1/7/2004				X			
Cyprus	23/11/2001	19/1/2005	1/5/2005				X			
Czech Republic	9/2/2005									
Denmark	22/4/2003	21/6/2005	1/10/2005		X		X	X		
Estonia	23/11/2001	12/5/2003	1/7/2004				X			
Finland	23/11/2001	24/5/2007	1/9/2007		X	X	X			
France	23/11/2001	10/1/2006	1/5/2006		X	X	X			
Georgia	1/4/2008									
Germany	23/11/2001	9/3/2009	1/7/2009		X	X	X			
Greece	23/11/2001									
Hungary	23/11/2001	4/12/2003	1/7/2004		X	X	X			
Iceland	30/11/2001	29/1/2007	1/5/2007		X		X			
Ireland	28/2/2002									
Italy	23/11/2001	5/6/2008	1/10/2008				X			
Latvia	5/5/2004	14/2/2007	1/6/2007		X		X			
Liechtenstein	17/11/2008									
Lithuania	23/6/2003	18/3/2004	1/7/2004		X	X	X			
Luxembourg	28/1/2003									
Malta	17/1/2002									
Moldova	23/11/2001	12/5/2009	1/9/2009			X	X	X		
Monaco										
Montenegro	7/4/2005	3/3/2010	1/7/2010	55	X		X			
Netherlands	23/11/2001	16/11/2006	1/3/2007				X	X		
Norway	23/11/2001	30/6/2006	1/10/2006		X	X	X			
Poland	23/11/2001									
Portugal	23/11/2001	24/3/2010	1/7/2010			X	X			
Romania	23/11/2001	12/5/2004	1/9/2004				X			
Russia										
San Marino										
Serbia	7/4/2005	14/4/2009	1/8/2009	55			X			
Slovakia	4/2/2005	8/1/2008	1/5/2008		X	X	X			
Slovenia	24/7/2002	8/9/2004	1/1/2005				X			
Spain	23/11/2001					X	X			
Sweden	23/11/2001									
Switzerland	23/11/2001									
The former Yugoslav Republic of Macedonia	23/11/2001	15/9/2004	1/1/2005				X			
Turkey										
Ukraine	23/11/2001	10/3/2006	1/7/2006		X		X			
United Kingdom	23/11/2001									

Non-member States of the Council of Europe

States	Signature	Ratification	Entry into force	Notes	R.	D.	A.	T.	C.	O.
Argentina										
Australia										
Canada	23/11/2001									
Chile										
Costa Rica										
Dominican Republic										
Japan	23/11/2001									
Mexico										
Philippines										
South Africa	23/11/2001									