Cyber Economic Crime and Commonwealth laws

Dr Clare Chambers-Jones
Associate Professor of Banking and Finance Law, University of the West of England & General Secretary of the Commonwealth Legal Education Association
Clare.chambers@uwe.ac.uk
@DocChambers
@CLEA1971

Abstract. The aim of this paper is to discuss the legal issues affecting commonwealth countries in terms of virtual/cyber financial crime. Virtual financial crime or cyber financial crime is where acts of fraud money laundering etc… take place over the internet. Virtual financial crime is a present and real threat to global economies and creating an international agreement to prevent, detect and punish virtual criminals is an increasing problem for governments and law enforcement agencies. This paper will consider the role of the Commonwealth in virtual financial crime and provide two cases studies, in part three, namely Australia and Nigeria, whose domestic jurisdictions aim to tackle cyber financial crime and how they draw upon commonwealth and international legislation for domestic purposes. It will discuss the jurisdictional elements in part four which the commonwealth should consider in line with more international laws. In the five part of the paper technological enforcements that can be used to prevent cybercrime will be examined. Finally the paper will use these commonwealth jurisdictions as an example of how global regulators could use it to promote a joined up response to virtual financial crime.

1. Introduction

Cybercrime can be described as any criminal activity having taken place via the internet, smart phone or other electronic means.1 Virtual financial crime is part of this cybercrime. It is where financial crimes such as fraud, money laundering, scams etc… take place on the internet. It is part of the cybercrime umbrella.2

Norton’s, the internet security software specialists in 2011 published a shocking report on the growth and impact of cybercrime. They report that cybercrime costs $388bn3 annually with 69%4 of adults having experienced some sort of cybercrime in their lifetime. The report also notes that people’s lives are increasingly becoming dominated by the internet with most adults spending 24 hours a week on the internet on average.6

4 Ibid.
5 Supra n.3.
6 Supra n.3.
One element of cybercrime which is pertinent to us for this paper is that of financial crime. Interpol acting to combat virtual financial crime states that, “the global nature of the Internet allows criminals to commit almost any illegal activity anywhere in the world, which makes it essential for all countries to adopt their domestic offline controls to cover crimes committed in cyberspace”. Therefore Interpol, the international law enforcement agency is stating that to combat this new wave of criminal activity domestic governments should tailor their domestic real world laws to fit the crimes that are being carried out in cyberspace. This has two important issues, firstly, they acknowledge that there is a real threat of financial crime being committed over the Internet and secondly, that because the virtual is a continuum of the real, domestic laws should be applied to the virtual worlds. However, this causes problems of its own. With the Internet crossing a multitude of boundaries and therefore laws, it is unclear as to which domestic law should apply in each instance of crime committed. There are no international standards, which have to be met. More discussion will be made on the international regulations further in the paper.

Given that cybercrime is a real threat to society we must explore the inherent aspect contained within money laundering and financial crime. To be able to commit virtual financial crime, as we use this as an overarching term for all financial crimes here, then real money must pass into the virtual ether and then be able to be extracted. Real money is therefore turned into virtual money. “Virtual money is defined as money value represented by a claim on the issuers which is stored on an electronic device and accepted as a means of payment by others persons other than the issuer”. Virtual money is therefore the digital currency which can then be used by the criminal to either launder, commit fraud. Virtual money can be said to be real money, it is an encrypted code representing money, which is accepted to be money. It is this same gradual acceptance by society, which ascribes the encrypted code as having monetary value.

2. Virtual Money Laundering

There are two types of virtual money; identified virtual money and anonymous virtual money. Identified virtual money is able to be identified as belonging to someone and that it was withdrawn from a banking institution. In other words it is traceable. Anonymous virtual money or what is known as virtual cash is untraceable. Once it is withdrawn it leaves no discernible trace. There are plentiful criminal activities which can then take place with this money. For example Interpol states that the main areas are:

- Unauthorised creation, transfer or redemption of virtual money;
- Criminal access to computer systems being used to change illicitly the attribution of funds within the system;
- Criminal attacks on virtual money systems leading to a loss of virtual money value or loss of function on the virtual money system;
- Criminal misuse of virtual money systems for financial crimes or as a tool to subvert or misuse other financial systems; and
- Criminals may use virtual money to reduce the likelihood of capture; for example, the cases of blackmail, kidnapping or extortion, where in the past,

---

collection of money has been problematic for perpetrators. This is particularly significant for anonymous virtual money.\textsuperscript{9}

So why is there virtual money in the first place? Virtual money was created along with the advancement of technology to create faster and more convenient ways of transferring money through commerce. In other words it is a development in the industrial world to do business. The Internet has now become a massive part of global commerce and where there is a means of conducting a criminal act, a criminal will exploit it and the Internet is of no exception.

The British Fraud Advisory Panel describe virtual money laundering as where; “A fraudster converts the proceeds of illegal activities into online currency, which is then used to purchase goods and/or services from you before being exchanged into real world currency.”\textsuperscript{10}

In the real world there are three stages to laundering money from illegal gains. These three stages are placing, layering and integration. The first stage, placing, is to put the money (which is normally cash) into a place such as a bank. In the case of virtual money laundering this could be a PayPal account as well. The second stage, layering, is to ensure that the money does not arouse suspicions. The criminal needs to carry out as many complicated and intricate transactions with the money so that any traces are hard to follow. The final stage, integration is where the criminal combines the so called dirty money with legitimate money, making the whole appearance of the money to be clean. From this very brief description you can already see how the virtual world, the virtual economy and the virtual money transfers lends itself to the criminal mind of laundering money. The dirty money can enter the virtual world through a pre-paid card, such as PayPal, where little identification is required. The money can be used to buy in world goods, through numerous accounts and then the criminal can sell these goods in world. The money from the investments in world can then be withdrawn from the world via an ATM or money account and the money appears to be from a legitimate source. It is therefore laundered.\textsuperscript{11}

Another element of economic cybercrime is fraud. Fraud, whether it is virtual or real, can lead to other criminal activities such as drug trafficking, people trafficking and terrorist financing. Other cybercrimes that are of interest are e-banking fraud and identity theft. The law in all these areas is falling behind the advancements in technology and there are little legislative provisions to combat these crimes. Furthermore without clear legislative provisions it is nearly impossible to quantify how prolific these crimes are.\textsuperscript{12}

\textsuperscript{9}Ibid.
3. Commonwealth and Financial Crime

The Commonwealth seeks to improve the legal provision of laws against cybercrime and in Perth 2011 an agenda was set to review cybercrime across the commonwealth. The Commonwealth Internet Governance Forum as well as the Commonwealth Secretariat is currently undertaking a cybercrime initiative project with various commonwealth stakeholders to commence work on promoting effective strategies to encourage safe and confident trade within the commonwealth. At the law ministers meeting in 2011, there was also the recognition that technology now presented a significant challenge to government, law and individuals and businesses alike. Furthermore the meeting acknowledged that the fast pace of the advancement of technology quickly overtakes the rigour and impact of the law.

Presently the law in the commonwealth which safeguards against cyber financial crime can be gauged from three pieces of legislation, namely:

- Commonwealth Model law On Computers and Computer Related Crime
- Budapest Convention of Cyber crime
- Scheme on Mutual Assistance in criminal Matters (Harare Principles)

3.1 Commonwealth Model law On Computers and Computer Related Crime (Model law) 2002

This piece of legislation is derived from the Council of Europe’s 2001 Convention on Cybercrime (Budapest Cyber Crime Convention) which is widely accepted as the most comprehensive international instrument present in today’s society on cybercrime. The model law is non-binding and provides a baseline for good practice for member state countries. Presently the UK, Australia and Canada have not signed up to the model law preferring their own domestic legislation as a means of legislative cybercrime.

The Model law is based on the assumption and acceptance of the increasing use of the internet for criminal activities. The Model law is divided into three parts, these being; part 1, the introduction, part 2, offences and part 3, procedural powers. The aim of the Act is to “protect the integrity of computer systems and the confidentiality, integrity and availability of data, prevent abuse of such systems and facilitate the gathering and use of electronic evidence”. Now ten years later, these aims of the Act seem very basic compared to the technological advancements of the internet and the criminal. Within part 1 of the Act various definitions are explained such as Computer data, computer data storage medium, and traffic data. Since the Act’s conception in 2002 advancements such as cloud computer, and portable memory sticks have come...
into being. The Act is phrased liberally and broadly enough to encompass these advancements in technology.

It is interesting to note that the Act when considering jurisdiction does specify that it has extended jurisdictional scope because of the very nature of internet activity. The jurisdiction goes a long way at creating cross jurisdictional links and provides guidance as to the interpretation of 'territorial jurisdiction' either through case law or the assumption of a substantial link to commonwealth or enacting country, thereby widening the jurisdictional impact of the Model law.

Part 2 lays out the offences under the Act. Section 5 states that illegal access of a computer system is punishable by imprisonment, a fine or both. Section 6 considers interfering with data to be punishable by imprisonment, a fine or both. Section 7, interfering with a computer system, is also punishable by imprisonment, a fine or both as are the offences of illegal inception of data (section 8), the use of illegal devices (section 9) and Section 10 child pornography. The Model law acknowledges the differences of law across the commonwealth on pornography and as such considers only child pornography within this legislation.

Part 3, procedural powers expands upon commonwealth countries already existing legislation or common law search powers already in existence. Sections 11 and 12 provide amendments to existing search powers to include search and seizure of computer systems. Section 13 of the Model law provides guidance as to the level of assistance the person who is subject to the search and seizure of Section 12, must provide. Section 14 outlines the police officers or equivalents obligation to create records of data and computer systems seized, with Section 15 outlining the remit of the magistrate to order the production of data from either the police or the Internet Service Provider. Section 16 and 17 related to the disclosure of stored data traffic and the preservation of data respectively. Section 18 and 19 allow magistrates, on reasonable grounds, to intercept electronic communication and traffic data. Section 20 considered that "in a proceeding for an offence against the law…the fact that a) it is alleged that an offence of interfering with a computer system has been committed; and b) evidence has been generated from that computer system; does not itself prevent that evidence from being admitted". Finally section 21 prevents Internet Service Providers from providing information pertinent to section 13, 15, 16, 17, 18 and 19, without lawful authority, and if this occurs it is punishable by imprisonment, a fine or both.

Although this is the first piece of commonwealth law on cybercrime it is now some ten years out of date and in need of reform and or modernisation. Aspects, such as virtual world crimes, online- gambling, copy right infringements (Art 10 of the Convention), and corporate liability (Art 12 of the Convention), add another layer of complexity to crimes committed on the internet are omitted from the Model law. Having said this though the model law is a good starting point for creating a more modern and up to date Model law.

---

18 Section 20 Model Law 2002.
3.2 Budapest Convention of Cybercrime

The Budapest Convention is the Council of Europe’s Convention on Cybercrime in 2001 and which provides the legislative background for the Model law (above). The Convention consists of 4 Chapter of 48 Articles. Many of which are comparable to the Model law. However, the European Convention provides more direct and in places, progressive legislative policies. For example, the Convention examines types of cybercrime such as Article 7, computer related forgery and Article 8, which relates to computer related fraud. The Convention also decrees on corporate liability something which the Model law shies away from- splitting the offences into computer relates offences and e-commerce offences (dealt with separately within the commonwealth). The convention also differs from the Model law on the grounds of outlining conditions and safeguards, in so much as the explicit affect to Article 15 (1) and the pursuant rights under the Council of Europe’s Convention for the Protection of Human Rights and Fundamental Freedoms, 1950, and the 1966 United Nations International Convention on Civil and Political Rights. If the commonwealth is to lead the way in combating cybercrime there needs to be recognition of these rights and procedures within any proposed future Model law.

Jurisdiction within the Convention has considerable parity with that of the Model law, in as far its legal phrasing and wide scope of jurisdiction. Within both the convention and Model law this is an important aspect of future legislative provisions given the complex and multi-jurisdictional nature of cybercrime. Article 25 and Article 31/33/34 also demonstrates the importance of international cooperation by laying down the remit of mutual assistance. The immediate assistance between countries as specified in Article 25 section 1-5 and Section 26 Section 1-2 provides for the co-operation between countries to counter the immediacy of the criminal act undertaken on the internet. Furthermore Article 35 provides for a 24/7 network point of contact to be available at all times for the purpose of immediate assistance to other jurisdictions. This legal provision is a feature of law which should be carried forward into any new reform legislation. It is also found in all three pieces of legislation laid out here.

This Convention is more comprehensive in nature than that of the Commonwealth Model law; however, the two combined provide a very powerful legislative statement of intent to provide a robust benchmark for cybercrime prevention.

3.3 Scheme on Mutual Assistance in criminal Matters (Harare Principles)

The Commonwealth has also produced what is known as the Harare Principles, which is a scheme for the mutual assistance on criminal matters. It was amended in 1990 at the Law Ministers Meeting, November 2002 and October 2005 and it brings together the logical and careful thinking of creating a mutual assistance law for commonwealth countries on criminal matters. It is important to consider within the context of cybercrime because of the criminal element of the offence. The Harare Principles are very comprehensive and being only 5 years old is much more modern and forward thinking, in terms of cyber and computer laws, than the Model law or the Convention.

---

Section 1(3)(a-j) sets out the areas in which competent authorities can provide assistance to other countries on criminal matters, for the purposes of cybercrimes, assistance can be sort on, identifying and locating of persons (a); search and seizure (d); obtaining evidence (e); tracing, seizing and confiscating the proceeds or instrumentalities of crime (i), and preserving computer data (j), to name just a few specific sections.

The scheme due its relative modernity compared to the other legislative provisions outlines comparatively up to date definitions under Section 4: Requests for computer data – definitions. The definitions are also in-depth and capture a wide remit of computer data available. This interpretation of the law also applies to Section 15 (1-5); requests for the preservation of computer data. Section 15 further to being more modern in its application than the Model law or the Convention it also is very prescriptive in terms of the requests for the preservation of computer data. Reading these sections in line with the Model law and the Convention allows for a more modernistic approach to be adopted by the legislator and judiciary in cases. The scheme also specifies like the Convention that a central authority (section 5) shall be designated for each country so that they can provide assistance at any time for cases falling under this scheme.

Section 8 of the scheme, refusal of assistance, provides guidance for a country who does not wish to assist in the request for assistance. The reasons for the lack of assistance in criminal matters if used for cybercrime cases could pose problems for reciprocity. Section 8(a) allows countries not to assist other countries if the crime committed in the requesting country is not considered a crime in the requested country. However most of the reasons for lack of assistance are fair and equitable in nature, for example Section 8 (2b), where assistance is allowed to be refused because of race, religion, nationality or political opinion. This is in line with the European Convention on Human Rights.

Also interesting to note is the confidentiality guidance under Section 11 whereby any requests made for assistance in any case shall be kept confidential. This is interesting because of the multi-jurisdictional issues of cybercrime. If there is an account of cybercrime being committed it is important to inform all possible jurisdictions of this in a timely fashion. By having confidentiality this would allow time to pass and jurisdictions not to take action.

Section 28 is important when considering cybercrime as it relates to the tracing of proceeds or instruments of crime. The scheme lays out that requests can be made to countries seeking assistance in identifying, locating and assessing proceeds or instruments of crime, (28(a)). This is important for law enforcement agencies to obtain this information and assistance in other jurisdictions because of the complexities of cross jurisdictional cybercrimes occurring.

Section 29, the seizure and confiscating the proceeds of instrumentalities of crimes does not make it clear whether it applies to financial proceeds but it can be read as if it could be applicable if ‘property’ is interpreted as including finance.

Section 32 provides for the assistance between countries on other matters not specifically prescribed within the scheme wording. This is a vital link between the scheme, the model law, the convention and cybercrime, when looking at future reforms of cyber law within the commonwealth.

The London Scheme for Extradition in the Commonwealth 2002 also adds a layer of mutual assistance for law enforcement agencies as the eliminative approach was adopted thereby ensuring rendition to be possible.

Within the next section of the paper a comparative analysis of two commonwealth countries will take place. These being Australia a developed country with a good level
of financial crime legislation and Nigeria, a developing country who are striving to eradicate the high levels of financial crime and corruption in the country. Transparency International, who monitors levels of corruption within countries have ranked Australia as 8th and Nigeria as 143rd in the world (1 being the best).\(^{22}\) PriceWaterhouseCoopers (PWC) 2011 Cybercrime report indicated that Australia reports 47% of cybercrime in 2011 compared to 40% in 2009. PWC also reported that Nigeria was among several countries that were perceived as potential countries where cybercrime could originate from. Perceptions as well as facts can be damaging to countries reputations as well as their economic outlook, therefore effective legislation prevention, deterring and detecting cybercrime is essential for not only developed countries but those developing too.

4. Case studies

4.1 Australia

Australia adopted in 2001 the Cyber Crime Act, the Cyber Crime Amendment Bill 2011 is being considered presently by the Australian government. The 2001 Act gives cybercrime a narrow definition with a wider definition pertaining from the European Convention on Cybercrime and as such the 2011 amendment Bill seeks to address some of the differences between the 2001 Act and the Convention, thereby falling under the umbrella of the law and Australia accession to this law. The bill makes amendments to the Telecommunications Act 1997, the telecommunications (Interception and Access) Act 1979, the Mutual Assistance in Criminal Matters Act 1987 and the Criminal Code Act 1995. The bill would allow Australia to come under the only international treaty on cybercrime presently. However Australia is also working with the commonwealth to provide legislative provisions against cybercrime.

In 2009 Australia launched a strategic framework to ensure commonwealth agencies work together in the prevention of organised crime. Cybercrime can now be seen as falling under the remit of organised crime and terrorism and therefore has always and especially since 9/11 and 7/7, taken seriously by governments and law enforcement agencies.\(^{23}\) The Australian Government’s adoption of the commonwealth strategic framework forged links between commonwealth agencies to prevent, disrupt, investigate and prosecute organised crime.\(^{24}\) The ideology of the initiative is to pool resources among commonwealth countries to fight cybercrime through fighting organised crime. Australia has also implemented additional legislative measures to combat serious and organised crime entitled, The Serious and Organised Crime Act 2010, does not mention cybercrime specifically however it can be interpreted widely enough to encompass cyber-criminal acts.


4.2 Nigeria

It is important for Nigeria to improve their image of being a hub for cybercrime, corruption and more general crimes. Nigeria is working hard at putting laws and agencies in place to prevent crime. As with other countries, Nigeria sees cybercrime as part of the overarching problems of organised crime and more specifically financial crime and money laundering. In 2005 the Financial Intelligence Unit (NFIU) in Combatting Financial Crime was created as part of the United National Convention Against Corruption Articles 14 and 58. The NFIU draws its powers from the Economic and Financial Crimes Commission (Establishment) Act 2004 and the Money Laundering (Prohibition) Act 2004. Neither of these Acts specifically mentions cybercrime.25 Instead the main instrument for tackling cybercrime is the Computer Security and Critical Information Infrastructure Protection Bill 2005, or the Cybercrime Bill. However, there are concerns that because the Bill does not distinguish between serious offences and minor misdemeanours that this could conflict with Article 37 of Nigeria’s constitution. Article 37 being the right to a private and family life whereby the Cybercrime Bill could interfere with people’s rights to privacy via the telephone and Internet. The bill also does not provide for independent monitoring of the agencies carrying out the provisions of the bill nor define the terms such as ‘law enforcement agencies’. The bill currently sits with the National Assembly and is still a long way off being implemented unless the various issues with the law can be rectified.

5. Jurisdictional Issues

The Internet has three levels of regulation, these being direct regulation of the Internet infrastructure itself; regulation of activities that can be conducted only over the Internet; and, regulation of activities which can be, but need not be, conducted over the Internet.26 According to Froomkin, the first sphere of direct regulation of the Internet infrastructure itself, includes: a. the standards of communication, b. the equipment used to provide and access Internet communication, c. intermediaries engaged in the provision of Internet communications, e.g. Internet Service Providers (ISPs).

The second sphere relates to the regulation of activities that can be conducted only over the Internet and which have no significant off-line analogues. The third sphere is where regulation takes place of activities which may or may not be conducted over the Internet, e.g. e-commerce in both tangible and intangible goods. This can be divided into categories too, for example some the Internet version of an activity may be regulated in a different way to an online version or that special regulation is devised because the use of the Internet makes existing rules impossible to implement such as e-cash or e-banking.27 It is therefore very difficult to come to a consensus nationally or internationally on what should or should not be implemented to regulate Internet activities. The regulations which are in place to regulate contractually activity on the Internet is as follows. Contractual activates are important here as this is where most of

27 Ibid.
the legislation is found due to the expanse of business and commerce via the net. We can draw inferences from the international cooperation in e-commerce situations and transpose these onto virtual economies.

In the EU, the UNICITRAL model law on Electronic Commerce and the UN Convention on the Use of Electronic Communications in International Contracts do not contain any jurisdiction provisions (Wang 2008). Furthermore the EC Directive on Electronic Commerce does not provide further clarification on private international law or court jurisdiction. The Brussels I Regulation, based on the old Brussels Convention does provide some remit of jurisdiction guidance in the absence of legislation in the EU. Article 2 of the Brussels I Regulation provides the general jurisdiction rule which states that any defendant who is domiciled in any one of the contracting states shall be sued at the place of their domicile. Therefore whether the person is an individual or a corporation Brussels I regulation provides this general jurisdiction based on domicile regardless of nationality. Article 5 provides the claimant with the opportunity to derogate from the general provision just mentioned and allows the defendant to be sued despite their domicile being outside the Member States. However, these are general considerations of jurisdiction under the banner of contract law and not criminal economic law. Within the US there are two types of jurisdiction, general and specific and as can be seen above is interpreted by the courts liberally.

The OECD is an "intergovernmental organisation whose purpose is to provide its 29 Member countries with a forum in which governments can compare their experiences, discuss the problems they share and seek solutions which can then be applied within their own national contexts". Chik believes that “the speed at which information technology has developed requires a faster, more reactive and automatic response for the law and that is not currently met by the existing law-making framework”. Chik therefore propounds a new method of law which is separate from private and public international law, that being customary international law. A term coined by using custom and practice as a means of agreeing on international standards of Internet regulation.

As can be seen above, the Commonwealth deals with relatively little of these issues within the Model law on cybercrime; the EU and UN protocols should be used as a starting point for the Commonwealth to create new jurisdictional depth to the Model law.

6. Technological enforcements

One way in which governments can control the access of its people to the Internet and the knowledge within is through technological enforcements and barriers. Reidenberg, as we have seen earlier in this paper, demonstrates the logical assumption that through the use of technological developments the government can use advances in technology to control and maintain legal enforcement. Technological barriers are just this. By

---

29 Recital 23 and Article 1(4) of Directive 2000/21/EC
30 Article 60 Brussels I Regulation.
having a technological barrier to all or some of the Internet governments can control or limit what people can see and use on the Internet and if a breach occurs then they have jurisdiction over their people. Many countries use this method of limitation as a method of maintaining jurisdiction. Within the UK the government has introduced the Digital Economy Bill 2011.33 The Bill is in response to the Digital Britain white paper (Cm 7650, June 2009) and the technological advancements in recent years. One of the most controversial elements of the Bill is to prevent illegal downloading and copyright infringement. The Bill states:

‘Internet service providers would have to cooperate with copyright owners to help curb illegal sharing or downloading of material, initially using a system of notification letters to users associated with repeated infringement. Copyright owners would be able to apply to a court to identify individuals suspected of more serious breaches thus aiding legal action using the current enforcement system. If these changes prove ineffective at reducing online piracy, the Bill would allow for the introduction of technical measures, including internet disconnection, to be used as a last resort against the most serious offenders.’

The Bill received Royal Assent in April 2010. However it has not been fully implemented as the UK government wait for the European Unions’ judicial review decision bought by two internet service providers who considered the provisions to be inconsistent with EU law and its provisions were disproportionate. It was held by Mr Justice Kenneth Parker that all but one of the arguments, relating to costs, was rejected.

This Act aims to ensure that ISP providers are responsible for what is happening throughout their networks. This would be regulated by OfCom, the independent regulator and competition authority for the UK communication industries.34 Although the government are enacting a technological border to inhibit and prevent illegal downloading and copy right infringement similarities can be drawn and assimilated for the purposes of virtual economic crime. The Act demonstrates the government intention to limit or prevent use of the Internet for criminals through restrictions on their ISP. As economic crime is a criminal offence a technological border could be imposed to prevent identified criminals from gaining access to the Internet. However with the use of Internet cafés and free wi-fi space people can gain free access to the Internet in most communal places. However, with careful thought on all aspects of the crime, technological borders can allow jurisdictional issues to be ratified against the rule of law. Reidenberg states that ‘for democratic societies, adherence to the rule of law means that the use of any technological enforcement instrument necessitates carefully prescribed authorisation criteria,’35 Furthermore the choice of the instrument used must be the ‘least intrusive to accomplish rule enforcement’.36 Reidenberg states that to ensure this is carried out four factors must be considered. These being: 1) a state must weigh the magnitude of any threat to public order; 2) the urgency of the threat must be considered; 3) the state must evaluate the effectiveness of the tool used, and 4) the state

34 For more visit: http://www.ofcom.org.uk/.
must consider the ultimately enforcement goal.\textsuperscript{37} Therefore if we consider this against the threat of economic crime and money laundering we can see that hypothetically speaking the government would see that economic crime and money laundering to be a great threat against public order. The urgency of the threat within the UK is present, real and highly likely and has been labelled by the Home Office as Severe.\textsuperscript{38} Therefore if this is a causal link between virtual money laundering and economic crime and terrorist financing and the likelihood of a terrorist attack occurring then we can see there is a need for technological barriers being in place even after stage two of the test. In the UK there is no tool being used to block terrorist financing through virtual economic crime, but should there be? If there is then it must also meet stage three of the test, that being to evaluate the effectiveness of the tool. In other words the tool must not prohibit any freedom of a person unless it is strictly necessary to directly prohibit economic crime. Any prohibitory tool must therefore be carefully designed and built into any technological blocking system. Should the UK, or any other country, use this method of enforcement then they must design the tool with the end enforcement goal in mind. The end goal is to prevent virtual money laundering and economic crime from occurring. A system must therefore be designed to prevent this. The end goal is to prevent terrorist financing as although a direct causal link to terrorist activities, economic crime is one step removed. The state must be careful to keep this consideration in mind so as to not to lose sight of the end goal. Terrorist financing is such an emotive subject that the end goal may be lost without careful and considered planning. Therefore any technological barriers must be implemented as a reaction to the problem but must be a well thought out and joined up strategy. Many considerations need to be taken into account and which have been highlighted already in this paper. However it is worth re-stating them here once more. Such consideration is whether each individual state applies jurisdiction and monitors and controls the situation within their own boundaries or whether there is an international plan agreed upon to combat economic crime globally.

Although the UK does not have an economic crime barrier in place the UK can and does use the Regulation of Investigatory Powers Act 2000 (RIAP). RIPA requires that when public authorities – such as the police or government departments – need to use covert techniques to obtain private information about someone, they do it in a way that is necessary, proportionate, and compatible with human rights.\textsuperscript{39} RIPA's guidelines and codes apply to actions such as:

- intercepting communications, such as the content of telephone calls, emails or letters.
- acquiring communications data – the ‘who, when and where’ of communications, such as a telephone billing or subscriber details.
- conducting covert surveillance, either in private premises or vehicles (intrusive surveillance) or in public places (directed surveillance).
- the use of covert human intelligence sources, such as informants or undercover officers.
- access to electronic data protected by encryption or passwords.\textsuperscript{40}

\textsuperscript{37} Supra n.35 pp.1964.
\textsuperscript{40} Ibid.
• Therefore in one way it could be said that the UK does play an important role in trying to combat economic crime, what is problematic for the crime agencies is that little is known about economic crime in virtual worlds and how to catch the criminals. Technology inhibits control in this instance. In other countries, for example the US, and Interpol, work is being done to monitor the situation and to provide technological solutions. The Commonwealth in line with this technological thinking could adopt procedures similar to this to provide technological barriers as a means of cybercrime prevention and detection.

7. **The future: International Laws of Cybercrime**

As iterated above there are presently three pieces of commonwealth law which guide countries on cybercrime. The Model law and the Convention are both relatively outdated and do not focus specifically on financial crime which is an ever increasing threat to the stability of the commonwealth economy and the confidence of the people of the commonwealth to conduct business over the internet. It is clear that cybercrime—whether it is economic and financial or people trafficking and more general organised crime—is a growing problem and one which crosses a plethora of jurisdictions. Therefore to be able to prevent cybercrime from increasing and from criminals increasing their hold over legitimate business then an international piece of legislation needs to be enacted to ensure reciprocity and cooperation between countries on cybercrime activities. The Model law on cybercrime goes some way to achieve this but it needs to be modernised. After the Commonwealth Ministers Meeting in Perth 2011 there is now an agenda to create such a law and steering groups are being created to commence the work needed to create such a law. The commonwealth has a breadth and depth of countries which would benefit from this Model law as can be seen from the struggles of not only Australia but Nigeria, as indicated above. It is not just the developed nations which need an international law but developing countries too. The commonwealth with its collegiate nature is the best possible place to commence this journey. However it is a journey which will not be easy for in 2010 Judge Stein Schjolberg proposed the “Cyberspace Treaty” to the United Nations, yet it was rejected. Schjolberg believes that the Convention of Cybercrime 2001 is based on criminal acts pertinent to the late 1990’s and as such is not suitable for crimes taking place in 2010’s. He draws upon the work of the International Law Commission which enacted the 1996 Draft Code of Crimes against Peace and Security of Mankind stating that serious crimes affecting the peace and security of mankind should be detailed as serious crimes against international law of cyberspace. Schjolberg further opines that international work was commenced in 2007 where the International Telecommunications Union (ITU) commenced the Global Cybercrime Agenda (GCA) which consisted of more than 100 experts in the area. Their report published in 2008 (with an update in 2009), stated that there were five main areas of work, these being:

• Legal measures,
• Technical and procedural measures,

42 Ibid.
43 Supra n.41.
• Organisational structures,
• Capacity building, and
• International Cooperation.

Schjolberg calls for not only there to be an International Treaty on Cyber security and cybercrime but also for there to be an International Criminal Court or Tribunal for cyberspace (ICTC).\textsuperscript{44} His work determines that although there are domestic laws in place as well as international and commonwealth laws these are out dated and cannot fight the increasingly advanced cybercrimes taking place in the 2010’s. He proposed therefore an International Treaty which has the standards and principles of the ‘European Cybercrime Convention 2001’ and also of the, ‘The European Convention of the Suppression of Terrorism 1977’.\textsuperscript{45} The reason for the use of the Terrorism Treaty is because, and Schjolberg denotes the divisions between terrorism and cybercrime, are becoming increasingly blurred and as there is not an internationally accepted definition of terrorism it is becoming harder to fight the criminal act when it is conducted over the internet.\textsuperscript{46}

The proposed Treaty on Cybercrime although debated at length was rejected by the United Nations because of countries reaching a stalemate in talks over the protection of national sovereignty and human rights.\textsuperscript{47} The idea of creating a global, international or even a commonwealth model law or treaty on cybercrime will always come up against resistance by domestic governments who do not agree on issues such as these mentioned above. Sovereignty and human rights play, rightly so, a huge role in creating the sanctity of nations, laws that transgress these state boundaries will cause disruption to these sacred national laws. To achieve an international agreement on cybercrime will take careful drafting, careful consideration of the laws within the parties countries. This is why the commonwealth, is in a solid position to create a model law on which future international laws can be based. The commonwealth, already shares many similar attributes, and this is not to say that the road to cohesion will be easy but it is a better starting place than that faced by the proposed treaty to the United Nations. The Commonwealth already has a Model law on cybercrime. It needs updating and modernising but the shared principles and standards of its constituent countries allow for the legislative path to begin in earnest.

\textsuperscript{44} Supra n.41.
\textsuperscript{46} Supra n.41.