SHOULD THERE BE A NEW BODY OF LAW FOR CYBER SPACE?

Doone Jones
University of South Australia , Adelaide, South Australia , Australia, jonda006@mymail.unisa.edu.au

Kim-Kwang Raymond Choo
University of South Australia, Adelaide , South Australia, Australia, raymond.choo@fulbrightmail.org

Doone Jones and Kim-Kwang Raymond Choo, 2014, "SHOULD THERE BE A NEW BODY OF LAW FOR CYBER SPACE?", Proceedings of the European Conference on Information Systems (ECIS) 2014, Tel Aviv, Israel, June 9-11, 2014, ISBN 978-0-9915567-0-0
http://aisel.aisnet.org/ecis2014/proceedings/track11/4

SHOULD THERE BE A NEW BODY OF LAW FOR CYBER SPACE?

Research in Progress

Jones, Doone, University of South Australia, Adelaide, Australia, jonda006@mymail.unisa.edu.au

Choo, Kim-Kwang Raymond, University of South Australia, Adelaide, Australia, Raymond.Choo@unisa.edu.au

Abstract

Malicious cyber activities are no longer a matter of if but of when, and in our increasingly interconnected world, threats to our national sovereignty can come from unexpected sources and directions – a 360-degree globalised challenge. Cyber security is no longer the preserve of any single country because of the trans-border nature of malicious cyber activities and an increasingly connected and sophisticated technological and user bases. The principle of territoriality, arguably, the 'bedrock' of criminal jurisdiction is central to the reason why trans-border malicious cyber activities are difficult to prosecute. At the very least, geographically based concepts of sovereignty must be 'squared' with the nature of open networks, possibly necessitating the development of a new law of cyber space to address the appearance of a lacuna in the law. In this paper, we seek to analyse the question "Whether there should there be a new body of law for cyber space?" by examining first the potentially broad application of jurisdictional criminal law, particularly the principle of extra-territorial jurisdiction, then if this hurdle is crossed, we then touch on what body of law should apply. We raise the notion that the conception of a new law of cyberspace and a forum for prosecution, is not impossible, but now is imperative.

Keywords: Cyber crime; Cyber space; Extra-territorial jurisdiction; International law of cyber space.

1 Introduction

What motivated this paper are the perceptions that municipal and international legal doctrine does not adequately deal with the problem of cyber crime; or, that no law is suitable; or, that the approach of retrofitting existing law to some cyber crime does not work; or, that even if jurisdiction and governing law are resolved, there is no global forum to enforce it.

We briefly discuss three fundamental steps required to prosecute cyber crime, namely jurisdiction, international governing law and forum. The idea is that if a state has the jurisdiction to prosecute, then the next questions are what law applies and, where it is enforced. We discuss extra territorial principles of international law as a jurisdictional basis for the prosecution of some cyber crime. We then reference briefly the obvious weakness of existing international legal doctrines of state responsibility, crimes against humanity and the law of armed conflict, in addressing the issue of cyber

crime statelessness and borderlessness. We finally draw the conclusion that there exists a precedent for establishing a forum to deal with criminals whose specific crimes were previously thought incapable of prosecution. We say learnings from this experience should be applied to cyber crimes that are described as 'grave'. 'Grave' because they threaten the 'well-being of the world'– see Rome Statute of the International Criminal Court (opened for signature 17 July 1988, 2187 UNTS 90, entered into force 1 July 2002, Preamble). It is first important to have a common understanding about why 'grave' cyber crime is out of the reach of municipal law.

2 The issue

The key issue in dealing with cyber crime now is in identifying answers to the questions: "Who is the perpetrator?" and "Where does the cyber crime originate?" (Choo 2014; Choo and Grabosky 2013). The technical and legal uncertainty surrounding these questions are why traditional boundaries are now blurred, because now it is not always possible to determine where the 'hardware and software of information and communications technology is located within national borders' (Bendiek 2014: 7). This is why we question whether the world can afford the 'legal and security responsibilities [to] remain within the jurisdiction of the nation-state' (Bendiek 2012: 12) for some cyber crimes, because the statistics point to how singularly unsuccessful this approach remains. But first, we move to describing aspects of borderless and stateless cyber crime.

2.1 What is cyber crime?

Malicious cyber activities can be broadly categorised into cyber crime, cyber war, cyber terrorism and cyber espionage. The Australian Government Attorney-General's Department (2009: 23) Cyber Security Strategy, for example, 'defines cyber crime as those computer offences under the *Criminal Code Act 1995* (Cth) that involve unauthorised access to, modification or impairment of electronic communications' (e.g. hacking, malware intrusions and denial of service attacks). Other definitions of cyber crime have included online fraud against individuals, businesses, and/or government agencies, illegal and inappropriate content (e.g. child abuse materials), online child/young people sexual exploitation (e.g. online child grooming), cyber bullying, and cyber stalking. However, it is the technical complexity with which cyber crimes are now masked that is the key issue. Threats are not clearly attributed to perpetrators, and it is this characteristic that disrupts what has been described as the traditional application internal or external state policies (Bendiek 2012). This masking lends itself to the ethereal concept of cyber space which also demands some attention.

2.2 What is cyber space?

The Council of Europe Convention on Cybercrime (the Convention) came into force in Australia, in accordance with section 3 of the *Cybercrime Legislation Amendment Act 2012* (Cth) (the Amending Act) on 1 March 2013. Not surprisingly, the Amending Act does not provide a definition of cyber space, or cyber crime, so for the purposes of this paper, it is assumed that the definition falls under the aegis of the Convention.

Cyberspace is characterised by the Convention as a place where cyberspace offences are committed against the confidentiality, integrity and availability of electronic building blocks (e.g. computer systems, traffic data and service providers) and is populated by actors. It may be characterised as borderless, anonymous, and, where there exists no 'rule of law' (Hooper, Martini and Choo 2013). As an aside, it is acknowledged that different states have 'different perceptions of the proper state-citizen relationship' (Bendiek 2014: 6). By way of clarification, we adopt the common law meaning of 'rule of law' in terms of the relationship of the individual with the state.

Perceptions of cyber space range from a global commons to an interstitial space (Manjikian 2010). Cyber space is both something and nothing. Controlling it is a proprietary preoccupation of states and criminals, where cyber offences are broadly based and have real world victims and perpetrators. It has been described as equivalent to the 'untamed American West' by Carr (2012). In cyber space, the roles of state and non-state actors have merged (Hollis 2007) which also means that the lines between cyber crime and cyber warfare are growing increasingly indistinct (Choo and Smith 2008).

Cyber warfare, or information operations / warfare, can now be conducted by both state and non-state actors (Hollis 2007). The latter includes transnational and terrorist elements targeting public or private interests. The key issue now is that the real world requires protection from cyber space (Manjikian 2010), and as will be shown below, existing international legal doctrine has inherent limitations.

2.3 What are the problems with the law?

The principle of territoriality, arguably the 'bedrock' of criminal jurisdiction (Bronitt and Gani 2003) is central to the reason why trans-border cyber crime, characterised since the 1990's by commentators such as Johnson and Post (1996) as inherently borderless, is so difficult to prosecute. At the very least, geographically based concepts of sovereignty must be 'squared' (Perritt Jnr 1996) with the nature of open networks and the blurring of the boundaries (Bendiek 2012) between municipal and international jurisdictional law. To that end, we focus specifically on two examples that demonstrate the extent of the breadth of an extra-territorial jurisdiction claim.

3 Is there jurisdiction to pursue 'grave' cyber crimes?

The short answer to the question is 'yes'. Jurisdiction may be understood in many ways, and is identified as three general types being the power of one State to perform acts in the territory of another (executive jurisdiction); the power of a State's courts to try cases involving a foreign element (judicial jurisdiction), and the power of a State to apply laws to cases involving a foreign element (legislative jurisdiction). Ordinarily, the issue is whether States are under a legal duty to recognise the exercise of jurisdiction by other States (Akehurst 1974). The second and third categories lay a foundation for potential disagreement between States, triggering respective bilateral or multilateral extradition treaties (Bantekas 2011) (for example, see Australia's *Mutual Assistance in Criminal Matters Act 1987* (Cth) and *Extradition Act 1988* (Cth)). If this trigger does not happen, or fails, then the next question is whether the extra-territorial application of law applies and in what circumstances. Below we look at the extent of US and Australian extra-territorial jurisdictional claims that are potentially available to those states, but first a word is necessary to describe the limitations of municipal law and why there is a need to look further afield into the international legal arena.

3.1 Terms explained

3.1.1 Municipal law

The term municipal law usually refers to the law that governs domestic aspects of national government whereas international law focuses on relations between states. This is 'an overly simplistic assertion' (Shaw 2008) because 'grave' cyber crime provides examples where the two systems clash. Municipal law is usually limited by territoriality and nationality principles which are explained as follows.

Bantekas (2011:4-5) explains that "territoriality is the simplest and least contentious form of criminal jurisdiction, even in respect of enforcement. It is generally established by the legislative and judicial practice of States in two alternative, but sometimes overlapping, ways. So-called subjective territorial

jurisdiction is asserted by those States in which criminal conduct commences on their territory, although the crime is ultimately consummated, or produces effects, in the territory of a third State. Equally, however, the State in the territory of which the effect was consummated has a legitimate interest in prosecuting the offenders. This interest will be exercised on the basis of so-called objective territorial jurisdiction. Case law suggests that this type of jurisdiction will be entertained where the criminal conduct has caused significant economic or other consequences within the territory of the affected State (*United States v Aluminium Co of America* [1945]; *Mannington Mills Inc v Congoleum Corp* [1979]). This corresponds to the effects doctrine, postulated by US courts, which was initially employed in anti-trust cases targeting cartels that threatened to harm rival US corporations. Following European protests over the far-reaching extraterritorial effects of the doctrine, it was held that jurisdiction under the doctrine had to be reasonable in that it should consider the economic interests of other States and the relationship between the US and the defendant (*Timberlane Lumber Co v Bank of America* [1976]). Objective territorial jurisdiction may also be justified on the basis of the continuing act doctrine, according to which a criminal act is not deemed to have ceased where it still produces results in the territory of a State. Transnational criminal conspiracies (Transnational Organized Crime) concerned with the trafficking of illicit substances or women and children (Narcotic Drugs and Psychotropic Substances; Human Trafficking) are by their very nature continuing crimes, and objective territorial jurisdiction is available to affected States (*Director of Public Prosecutions v Doot* UKHL [1973] 1 All ER 940)."

Bantekas (2011: 13) further explains that "the nationality principle confers on States the power to subject their own nationals to judicial and legislative criminal jurisdiction for crimes they have committed abroad. The mere fact of nationality does not give rise to this type of jurisdiction in respect of all crimes committed abroad; rather, it has to be preceded either by particular or general criminal legislation, otherwise it may be deemed to offend the principle against the application of retroactive legislation – *Nulla poena nullum crimen sine lege*. Increasingly, the contemporary trend in justifying the exercise of nationality jurisdiction by developed States is the avoidance of impunity in respect of certain countries where particular behaviour is either not qualified as criminal, or even if it is the authorities generally fail to prosecute the offenders".

3.1.2 Extra-territorial jurisdiction

The complex operation of territorial and extra-territorial jurisdiction is further explained by the Council of Europe, as follows:

> *For the purpose of allowing the exercise of jurisdiction in accordance with the principle of territoriality, the place of commission is determined on the basis of what is known as the doctrine of ubiquity: it means that an offence as a whole may be considered to have been committed in the place where a part of it has been committed. Some states categorise the acts, others their effects. Because of that dual categorisation, it is possible for states to claim territorial jurisdiction. As a result, it is quite possible that several states consider themselves empowered, on the basis of the territoriality principle, to take cognisance of the same offence. According to one form of the doctrine of ubiquity, an offence may be considered to have been committed in the place where the consequences or effects of the offence become manifest. This doctrine of effects is accepted in several member states; not all of them require that the offender must have intended the effects of his acts to occur in the territory of the state claiming jurisdiction. Questions concerning the implication of extraterritorial elements in criminal acts have been recognised in connection with participation, procuring the commission of an offence, attempted offences, planning an offence, offences of omission, continuous offences, a series of offences violating several legal interests, and connected offences. (Council of Europe 1992)*

Extra-territorial jurisdiction also falls under these categories namely, the principle of the nationality of the offender, the principle of the flag, the principle of the nationality of the victim, the principle of

protection, the "representation" principle, the principle of universality, and forms of extraterritorial jurisdiction which do not fall under the aforementioned categories (Council of Europe 1992).

3.2 US application of the extra-territorial jurisdiction

We observe that the US application of extra-territorial jurisdiction appears to be exceptionally broad. The US Department of Justice Computer Crime and Intellectual Property Division states that:

> *[a]bsent evidence of a contrary intent, the laws of the United States are presumed not to have extraterritorial application. See United States v. Cotten, 471 F.2d 744, 750 (9th Cir. 1973). The prosecution may overcome this presumption against extraterritoriality by showing "clear evidence of congressional intent to apply a statute beyond our borders." United States v. Gatlin, 216 F.3d 207, 211 (2d Cir. 2000) (internal quotations omitted). "Congress has the authority to enforce its laws beyond the territorial boundaries of the United States. Whether Congress has in fact exercised that authority in [a particular case] is a matter of statutory construction." Equal Employment Opportunity Comm. v. Arabian American Oil Co., 499 U.S. 244, 248 (1991)" (internal citations omitted). Further, "[e]xtraterritorial jurisdiction may exist not only based on specific Congressional intent, but also based on intended and actual detrimental effects within the United States. "The intent to cause effects within the United States . . . makes it reasonable to apply to persons outside United States territory a statute which is not extraterritorial in scope. (United States v. Muench, 694 F.2d 28 33 (2d Cir. 1982)). (US DoJ n/y: 115).*

The salient point here is that this US position is a very broad application of the 'effects' doctrine previously described by commentators (Bantekas 2011; Johnson and Post 1996), and the Council of Europe (1992). The US position also implies that the US policy is not only driven by 'the military logic of deterrence which entails maintaining and strengthening an offensive capacity' (Bendiek 2014: 4) but has, arguably, a much broader application potentially to borderless or stateless cyber crime.

3.3 Australian application of extended geographical jurisdiction (extra-territorial)

We observe in Australia, that extra-territorial jurisdiction is not an unfamiliar concept both in terms of legislative response and is expressed in the term 'extended geographical jurisdiction'. In *Lipohar v The Queen* (1999) 200 CLR 485, Gleeson CJ stated in obiter, "[t]here is nothing new about trans jurisdictional activity giving rise to potential breaches of the laws of a number of territories. As La Forest J pointed out in Libman, developments in communication by post and telegraph more than a century ago gave rise to such problems".

In Australia, extra-territorial jurisdiction has four categories in the *Criminal Code Act 1995* (Cth). Comment on category D is that it provides for offences to anyone anywhere regardless of citizenship or residence and regardless of whether the conduct involved is not unlawful in the other country in which it occurs (Odgers 2010). Category D offences are, therefore, in a black letter law sense, unrestricted. The *Criminal Code Act 1995* (Cth) applies category D extended geographical jurisdiction to crimes of treason and urging violence, offences relating to espionage and similar activities, terrorism, the proper administration of government, and theft of Commonwealth property. One point about Australian law is that "Parliament cannot recite itself into a field the gates of which are locked against it by superior law" (*The Australian Communist Party Case* (1951) 83 CLR 1 (Fullagar J)). In other words, just because a law exists does not mean it is not ultra vires, as the Commonwealth only receives its power from the *Constitution of Australia Act 1901* (Cth). The law must be constitutionally valid for the Commonwealth to apply it. The point here is that even applying a broad interpretation of extra-territorial jurisdiction, the external affairs power has some constitutional limit in Australia. This compares with the United States, which appears limitless, as seen below.

4 Summary: What law applies?

If a broad application of jurisdictional principles is accepted, then what law should apply? Bodies of law such as the law of armed conflict, state responsibility and international humanitarian law we consider in more detail in the extended version of this paper, but in summary they all have varying reliance on the territorial nexus of the known attacker. For example, a media report indicates that on 7 June 2013, agreement was reached between US, Russia and China, that the international "law of state responsibility applies to cyberspace which means states must hold non-state actors – terrorists, criminals, and activist hackers –accountable for wrongful acts in cyberspace that originate from the states territory ... states should not use these actors to commit wrongful acts in cyberspace on their behalf ... the goal is to consider what norms should apply below the level of armed conflict in cyberspace" (Farnsworth 2013, np). There have, however, been conflicting media reports giving the appearance that the superpowers of the world appear to have settled on a legal doctrine heeding calls for the development of new norms of state behaviour in cyber space. One key message is these superpowers have focussed attention on the international doctrine of state responsibility as one way forward, rather than armed conflict, but problems with attribution remain.

Back in the 1990s, the discussion was prolific about the merits of a new law of cyberspace. Commentators such as Perritt Jnr (1996) were concerned with the inadequacies of civil, criminal, commercial and international law because of the lack of capacity to deal with cyberspace procedurally, choice of law enforcement of judgments, and discovery. These writings also struggles with the complexities of where a 'law of cyberspace' might come from, and whether it should have either a self-regulated decentralised approach, reflecting the model of the internet, or adopt a centralised approach which sat more comfortably with the notions of state control and sovereignty. There were also the regulation "skeptics" (Goldsmith 1998) and those who believed in a systems and architecture type of control (i.e. through code – see Lessig 1996). The extension of Lessig's theory in 'lex informatica' (Reidenberg 1998) was based on a system of virtual courts of self-enforcement, attempting to overcome geographical boundaries, but suffering from the questions surrounding centralised control. The chilling point about lex informatica is the way the control of the cyber space architecture might play such a significant legal role for both state and non-state actors. For instance, would it be for organisations (and not states) to determine all packet switching, or internet browsing and internet searching (Mayer-Schönberger 2008). The rise of proprietary empires controlling the Internet is a theme revisited in 2012 (Perritt Jnr 2012).

None of these approaches solves the problem, and to that end the solution now can only come from a reconceptualization of legal thinking of governing law in this area. The process of completely rethinking transnational crime, perpetrators and their apparent immunity from prosecution, has been done before. For instance, the precedent is that crimes against humanity are now defined and, a court built for their prosecution. The task of developing a new law for cyberspace for 'grave' borderless and stateless cyber crime is therefore imperative, but not impossible.

References

Akehurst, M. (1974). Jurisdiction in international law. British Yearbook of International Law, 46, 145-257.

Bantekas, I. (2011). Criminal jurisdiction of states under international law. Max Planck Encyclopedia of Public International Law.

Bendiek, A. (2012). European cyber security policy. SWP Research Paper 13, Berlin, Germany: German Institute for International and Security Affairs.

Bendiek, A. (2014). Tests of partnership. SWP Research Paper 5, Berlin, Germany: German Institute for International and Security Affairs.

Bronitt, S. and Gani, M. (2003). Shifting boundaries of cybercrime: From computer hacking to cyber-terrorist. Criminal Law Journal, 27(6), 303-310.
Carr, J. (2012). Inside cyber warfare, 2nd ed. O'Reilly.
Choo, K.K.R. (2014). A conceptual interdisciplinary plug-and-play cyber security framework. In Kaur, H. and Tao, X., eds, ICTs and the Millennium Development Goals – A United Nations Perspective, New York, USA: Springer.
Choo, K.K.R. and Grabosky, P. (2013). Cyber crime. In Paoli, L., ed, Oxford Handbook of Organized Crime, Oxford University Press.
Choo, K.K.R. and Smith, R.G. (2008). Criminal exploitation of online systems by organised crime groups. Asian Journal of Criminology, 3(1) 37-59.
Council of Europe. (1992). Extraterritorial criminal jurisdiction. Criminal Law Forum, 3(3), 441-480.
Farnsworth, T. (2013). Expert group coalesces on cyberspace. Arms Control Today, July/August.
Hooper, C., Martini, B. and Choo K.K.R. (2013). Cloud computing and its implications for cybercrime investigations in Australia. Computer Law and Security Review, 29(2), 152-163.
Hollis, D.B. (2007). Why states need an international law for information operations. Lewis & Clark Law Review, 11(4), 1030-1033.
Johnson, D.R. and Post, D. (1996). Law and borders – The rise of law in cyberspace. Stanford Law Review, 48(5), 1367-1402.
Lessig, L. (1996). The zones of cyberspace. Stanford Law Review, 48, 1403-1411.
Manjikian, M.M. (2010). From global village to virtual battlespace: The colonizing of the internet and the extension of realpolitik. International Studies Quarterly, 381(2), 389-391.
Mayer-Schönberger, V. (2008). Demystifying Lessig. Wisconsin Law Review,4, 713-746
Perritt Jnr, H.H. (1996). Jurisdiction in cyberspace. Villanova Law Review, 41(1), 1-128.
Perritt Jnr, H.H. (2012). The internet at 20: Evolution of a constitution for cyberspace. William and Mary Bill of Rights Journal, 20(4), 1115-1180.
Odgers, S. (2010). Principles of federal criminal law, 2nd ed, Thomson Reuters.
Reidenberg, J.R. (1998). Lex informatica: The formulation of information policy rules through technology. Texas Law Review, 78(3), 553-566.
Shaw, M.N. (2008). International law, 6th ed. Cambridge University Press.
United States Department of Justice (US DoJ) (n/y). Prosecuting computer crimes. http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf