

Broadhurst, R.G., 2006, 'Content Cybercrimes: Criminality and Censorship in Asia'  
*Indian Journal of Criminology*, Vol 34 (1&2):11-30.

Revised draft working paper 22.11.04

### ***Content Cyber-Crimes: Criminality and Censorship in Asia***

Roderic Broadhurst, University of Hong Kong\*

\*Associate Professor, Department of Sociology, The University of Hong Kong, Pokfulam, Hong Kong, email: broadie@hkucc.hku.hk. An earlier draft was presented at the Council of Europe Conference on Cyber-Crime, Strasbourg, 15–17 September 2004.

#### **[A] Introduction<sup>1</sup>**

Information technologies and computer connectivity, especially via the Internet, have radically changed the way the world communicates and help to drive the processes of 'globalisation'. Time and space are seemingly compressed (the 'death of distance'<sup>2</sup>) and new 'digital' economies emerge while markets (legal or illegal) exploit opportunities and create wealth, while governments grapple with policing the 'information super-highways'. Digital divides have also emerged, with many less developed countries excluded from competing in this new world, to the disadvantage of their economies.<sup>3</sup> The digital divide also has consequences for the effective global enforcement of cyber-crimes: undeveloped and vulnerable IT national infrastructures, coupled with weak IT security and

---

<sup>1</sup> The author is grateful to Senior Inspector Frank Law of the Technology Crime Division of the Hong Kong Police for information relating to 'content' cyber-crime cases and Dr Lena Zhong for a web search and the translation of Chinese websites.

<sup>2</sup> On April 23, 1838 15 days after leaving London the steam ship *Great Western* arrived in New York breaking the cross-Atlantic and the city was greeted the next day with the newspaper headlines 'Annihilation of Space and Time' the average sailing vessel required usually about 40 days for the westward passage although the record for the westward passage by mail packet was 17 1/2 days: Fishlock, T. 2004. *Conquerors of Time*, John Murray: London, p168.

<sup>3</sup> Norris notes that there are many divides between developed and developing nations, social divides between the information-rich and poor and differences in the way the technologies are used to enhance political participation; see P. Norris (2001). *The Digital Divide: Civic Engagement, Information Poverty and the Internet Worldwide*. Cambridge University Press.

policing, provide 'safe havens' and crime 'rookeries'. As sociologists have recognised, 'communities of shared fate', not necessarily contiguous with nation-states, have now emerged and the failure of one to act against crime is sufficient to nullify the positive actions of others. Without a seamless web of mutual legal assistance and comity between nations, and without public/private partnerships, policing the information superhighway will be impossible and the 'frontier' of cyberspace will be as lawless as any wild west.

Advocates of a 'free' Internet who suggest that it both encourages civil society and enhances the democratisation of otherwise authoritarian regimes have been challenged.<sup>4</sup> There is little evidence that the Internet has undermined authoritarian regimes<sup>5</sup> or has developed faster in those jurisdictions with higher literacy levels, political freedom and English proficiency in Asia.<sup>6</sup> The Internet's capability as a profound and vibrant vector of free speech is well known, as is its attraction to the purveyors of hate, sadistic erotica and child pornography and other menaces whose markets are readily cultivated and exploited. The Internet is a market open to all with access to a computer and something to say or sell, though there is little evidence that it is awash with 'snuff movies', hate sites, child pornography or DIY bomb guides. (Recent, if contentious, estimates suggest as little as 5% of the several million web-pages on the Internet are 'Adult'.<sup>7</sup>)

Neither cyber-patrolling, automated web-search crawlers or self-regulatory codes can capture or suppress the near infinite variety of harmful content now present on the Internet or communicated via its exponential connectivity. Nevertheless the struggle for social control over this crucial vector of modernity has yet to meet the test of sufficient consensus about what kind of 'speech' harms matter and the means to prevent it. Activation of law enforcement and the criminalisation of so-called 'content' cyber-crimes are but one approach, often drawn upon because of the presumed deterrent and educative role of the law. But the success and credibility of extremist websites is usually achieved when watchdog groups or law enforcement seek to shut them down. The success of a website depends on its 'stickiness' (i.e. the retention of the web-visitor) but often at the cost of credibility. The perceived credibility of a website is usually related to the number of non-self-

---

<sup>4</sup> N. Hara & Z. Estrada (2003). Hate and peace in a connected world: comparing MoveOn and Stormfront. *First Monday*, 8(12). [[www.firstmonday.org/issues/issue8\\_12/hara/index.html](http://www.firstmonday.org/issues/issue8_12/hara/index.html)]

<sup>5</sup> S. Kalathil & T.C. Boas (2001). The Internet and state control in authoritarian regimes: China, Cuba and the counterrevolution. *First Monday*, 6(8). [[www.firstmonday.org/issues/issue6\\_8/hara/index.html](http://www.firstmonday.org/issues/issue6_8/hara/index.html)]

<sup>6</sup> X.M. Hao & S.K. Chow (2004). Factors affecting Internet development: an Asian survey. *First Monday*, 9(2). [[www.firstmonday.org/issues/issue9\\_2/hara/index.html](http://www.firstmonday.org/issues/issue9_2/hara/index.html)]

<sup>7</sup> The much-cited Marty Rimm study published by *Time* in 1995 which claimed 83.5% of all images on the Internet were 'Adult' has been soundly criticised; see <[www.caslon.com.au/censorshipguide2.htm](http://www.caslon.com.au/censorshipguide2.htm)> and <[www.caslon.com.au/xcontentprofile.htm](http://www.caslon.com.au/xcontentprofile.htm)>.

referential links it provides, though most hate sites rely on retaining visitors by providing links that are self-referential.

One aspect of cyber-crimes less easy to grasp than the far too common events of identify theft, malicious and exploit code, and fraud offences is the problem of ‘content’ crimes. Content crimes are not clearly defined and are a heterogeneous category, but the term is often meant to refer to the ‘undesired’ and illegal substance of an image or text communicated via computers and the Internet. It appears that content crime equates with the dissemination of offensive materials: pornography/child pornography; online gaming/betting; racist material; and treasonous or sacrilegious material. It also may include the activities of stalkers or harassers that target victims via e-mail. For practical purposes the notion of content crime does not usually include the creation of counterfeit or surrogate identities, misleading advertising and other deliberately deceptive representations with fraudulent purposes – although all of these may play some part in the substance of web-pages, spam (as in the case of the ‘419’ frauds) or other communications content that have been criminalised.

#### **[A] ‘Content’ offences and the Council of Europe Additional Protocol**

Only a few specific content offences have been criminalised. The best known and most universal of these relate to the production and distribution of child pornography, the promotion of or trafficking in narcotic and psychotropic drugs, hate or racial/ethnic vilification crimes and, in Europe at least, gross denials of genocide episodes. The Council of Europe (CoE) Cyber-crime Convention that came into force in early 2004 is one of the first international treaties to criminalise the distribution of child pornography via computers, so this is one of the few content crimes to attract widespread consensus.<sup>8</sup> This provision reinforces the ‘Optional Protocol to the Convention on the Rights of the Child’ on the sale of children, child prostitution and child pornography approved in the May 2000 session of the UN General Assembly.<sup>9</sup> Although the Cyber-crime Convention has developed an Additional Protocol signed by 23 nations addressing racial/ethnic vilification and genocide denial,

---

<sup>8</sup> Child pornography is the only ‘content’ offence cited by the Transnational Crime Working Group of CSCAP (Council for Security Cooperation Asia Pacific) in its report *Cyber-crime and its Effects on the Asia Pacific Region*; see 4 August, at <[http://www.police.govt.nz/events/2001/e-crime-forum/cybercrime\\_and\\_its\\_effects.html](http://www.police.govt.nz/events/2001/e-crime-forum/cybercrime_and_its_effects.html)>.

<sup>9</sup> The optional protocol was signed by PR China on 6 September 2000 and ratified by the National People’s Congress Standing Committee on 29 August 2002.

this is yet to be ratified. The aim is to harmonise substantive criminal law in the fight against racism and xenophobia on the Internet and improve international cooperation in this area.<sup>10</sup>

The Additional Protocol specifies the putative criminal offence of dissemination of racist and xenophobic material through computer systems via threat or insult – where public insult of a person or group of persons occurs because they belong to or are thought to belong to a group distinguished by specific characteristics. ‘Insult’ refers to any offensive, contemptuous or invective expression that prejudices the honour or dignity of a person, and such expression is directly connected with the insulted person’s belonging to the group. Unlike threats, an insult expressed in private communications is not outlawed, presumably on the practical grounds that ‘thoughts’ cannot be policed. In short, there is a distinction between ‘abusive expression’ and ‘offensive expression’, the former targeting persons, the latter ideas.<sup>11</sup>

In addition, the denial, gross minimisation, approval or justification of genocide or crimes against humanity is also criminalised. These behaviours have also inspired, stimulated and encouraged racist and xenophobic groups and are not limited to Nazi atrocities but include serious crimes against humanity established by other international courts set up since 1945 by relevant international law (such as UN Security Council Resolutions and multilateral treaties).<sup>12</sup> This Article allows reference to final and binding decisions of future international courts recognised by the parties to the Protocol. The provision is intended to ensure that established historical facts may not be denied, grossly minimised, approved or justified in order to support racist and xenophobic ideologies and

---

<sup>10</sup> The definition of content refers to written material (e.g. texts, books, magazines, statements, messages), images (e.g. pictures, photos, drawings) or any other representation of thoughts or theories, of a racist and xenophobic nature, in such a format that it can be stored, processed and transmitted by means of a computer system. The definition contained in the Protocol refers to conduct that may arise from the content of the material rather than to the expression of feelings or belief or aversion alone. The conduct involved must also be done ‘without right’ and may be lawful not only in cases where classical legal defences like consent, self-defence or necessity apply, but where other principles limit liability (e.g. for law enforcement, academic or research purposes). The Protocol excludes conduct undertaken by lawful government authority (e.g. where government acts to maintain public order, protect national security or investigate criminal offences). Offences must also be committed ‘intentionally’ for criminal liability to apply, although ‘intention’ is left to national interpretation. Thus an ISP cannot be held criminally liable merely because it served as a conduit for offensive material, or hosted a website or newsroom containing such material, without the required intent under domestic law, and an ISP is not required to monitor such conduct to avoid criminal liability. See G. Esposito. (2004). *The Council of Europe Convention on Cyber-crime: A Revolutionary Instrument?* In R. Broadhurst (Ed.). *Proceedings of the 2nd Asia Cyber Crime Summit*. Centre for Criminology: University of Hong Kong.

<sup>11</sup> As per the argument of L. McNamara (2002). *Regulating racism: Racial vilification laws in Australia*. Sydney: Federation Press; see also J. Jacobs & K. Potter (1998). *Hate Crimes: Criminal Law and Identity Politics*, Oxford University Press.

<sup>12</sup> For example, the International Criminal Tribunals for the former Yugoslavia, the Permanent International Criminal Court for Rwanda as well as the International Military Tribunal, established by the 1945 London Agreement.

behaviour.<sup>13</sup> Like the US 1999 *Hate Crime Prevention Act*, such attempts at criminalisation are likely to face numerous challenges through the courts. White supremacist websites such as ‘Stormfront’, ‘Front14’ and others of this ilk may skirt these conditions and continue to proliferate<sup>14</sup> – although Yahoo and French ISPs may have seen business interests at risk rather than censorship as the motive for desisting with accounts of the ‘Front14’ kind.

The Chinese have repeatedly demanded that the Japanese authorities undertake measures to suppress the not infrequent cases of what they regard as historical misrepresentations of the 1937–45 Sino-Japanese war that appear both in academic texts and ultra-nationalist Japanese websites. Most sensitive of these misrepresentations is the outright denial or underplay of the notorious massacre of Nanjing in 1937 – by conservative estimates 200,000 Chinese citizens were murdered by rampant Japanese Imperial troops after the occupation of the city.<sup>15</sup> The Shinto Yasukuni (‘peaceful country’) Shrine located in Tokyo and founded in 1869 to commemorate Japan’s war dead<sup>16</sup> has also become a source of controversy since 1978 when 14 class A war criminals were enshrined among the 2.5 million war dead. Periodic visits to the shrine by several Japanese prime ministers, including the current incumbent, have caused concerns within Japan as a violation of the constitutional separation of church and state. For Asian countries, particularly China, the shrine has become a symbol of Japanese militarism and ultra-nationalism, and prime ministerial visits are perceived as a form of genocide denial.<sup>17</sup>

Unlike China, Japan (one of the four nations outside the Council of Europe who participated in the drafting of the Convention) is a signatory to the Convention, but Japan is yet to consider the Additional Protocol.<sup>18</sup> The Protocol is a mechanism that may offer some prospect of curtailing the more virulent forms of denial emanating from xenophobic groups in Japan and in China, where

---

<sup>13</sup> Paraphrased from Esposito, *The Council of Europe Convention on Cyber-crime*.

<sup>14</sup> See HateWatch.org and the Simon Wiesenthal Centre estimated there were 3000 problematic Internet sites in 2002 and the Southern Poverty Law Centre noted 405 extremists; see Hara & Estrada, *Hate and peace in a connected world*.

<sup>15</sup> See Takeshi Yoshida (1999). *A Japanese Historiography of the Nanjing Massacre*, <<http://www.columbia.edu/cu/ccba/cear/issues/fall99/text-only/yoshida.htm>>.

<sup>16</sup> The deities of about 2.5 million people who died serving Japan in domestic and overseas conflicts including the Meiji Restoration, the Satsuma Rebellion and other domestic conflicts, the First Sino-Japanese War, the Russo-Japanese War, the First World War, the Manchurian Incident, the Second Sino-Japanese War and the Pacific War are enshrined at Yasukuni Shrine in the form of mortuary tablets. The Yushukan, a museum commemorating Japan’s wars, is located next to the shrine’s main buildings.

<sup>17</sup> Attempts to solve the problem by creating an alternative shrine for Japan’s war dead or by removing the war criminals from the Yasukuni Shrine have failed due to the refusal of its Shinto guardians to relinquish a national tradition.

<sup>18</sup> There are at present 23 signatories to the additional protocol but as yet no ratification; see <[conventions.coe.int/Treaty](http://conventions.coe.int/Treaty)>.

distinct anti-Japanese rhetoric can reach the level of vilification as in <www.japanpig.com>, the website of the 'anti-Japan pioneers'.<sup>19</sup> Even a cursory inspection of bulletin boards and chat rooms would have noted strident anti-Japanese sentiments during the August 2004 Asian Football Cup held in Beijing. In both jurisdictions, 'hactivism' has been one of the consequences of the unresolved tensions. There is even an anti-Japan virus, a derivation of W32-Welchita-B that targets computer systems in Japanese but not those in Chinese, Korean or English; this same 'anti-Japanese virus' downloads helpful Microsoft patches.

The UN Transnational Organised Crime Convention (in force from September 2003) also universally criminalised those who use computers to organise the smuggling of humans or the exploitation of woman and children (sex slavery), and the trafficking of firearms and explosives (awaiting ratification) or the pursuit of serious organised crime are also universally deplored and subject to sanction. Presumably communications containing content in respect to these activities are equally subject to law enforcement.

Websites devoted to terrorism as well as those devoted to fraud apply deceptive content (as in the substance of their text and imagery) to enable their anonymous operators to justify murder or commit theft. Is the creator of a website or a spammer who displays a video of an execution (unlawful or lawful) or offers miracle cures, promotes euthanasia, provides games of chance or sells unusual and sadistic erotica committing a 'content' crime? The definition of what constitutes crime is essentially a political process and the answer to questions of this kind ultimately rests on the political responses that are mobilised by ('moral panics' or otherwise) the social values and interests that are offended.

This paper briefly explores the issue of 'content' cyber-crime in the Asian context and discusses the likely response to the problems of deviant expression on the Internet. Although censorship backed with sanctions, the usual response to the problem of 'content' crime', is anathema to the utopian architects of the Internet, this should not imply that web-pages or mass spam attachments are any different from print media and therefore outside the standards normally applied to the mass media.

---

<sup>19</sup> The homepage features a photo of an entertainment centre in Xiangtan, Hunan (Chairman Mao's hometown), which has a statue of a kneeling Japanese soldier with a sign saying 'bad Japanese are not welcome'.

## [A] Context

Although data on uptake and penetration of computer connectivity and Internet growth in Asia are subject to estimation errors and are rapidly outdated, there were an estimated 64 million Internet users in Asia in 2000,<sup>20</sup> expected to reach 242 million by 2005.<sup>21</sup> According to the International Data Corporation, between 1998 and 2003 Asia as a whole saw a compound annual growth rate in Internet users of 40%, with India (76%), China (51%) and South Korea (49%) leading.<sup>22</sup> China in 2002 had 56.6 million people, increasing to 87 million by mid-2004,<sup>23</sup> who could access the Web from their home, overtaking Japan as the largest group in Asia. Chinese access has been optimistically estimated to reach 257 million or 20% of Chinese households by the close of 2006 – exceeding numbers estimated in North America.<sup>24</sup> According to CNNIC's '14<sup>th</sup> Statistical Report on Internet Development in China', as of mid-2004 China had 36.3 million hosts, 382, 216 CN domain names, 6.27 million WWW sites, 31.1 million broadband users and the widespread uptake of a full range of services (e.g. search engines, online banking, auctions, advertising, online news and VOD, e-mail, SMS etc.), while 38% of the population have used the Internet to make online purchases.<sup>25</sup> Hong Kong also has a high percentage of Internet users, with 64.1% of local households connected to the Internet. Singapore (55.6%), South Korea (52.7%), Taiwan (49.8%) and Japan (48%) have the highest level of Internet penetration and only Myanmar remains to provide public access to the Internet (see Table 1).<sup>26</sup>

**Table 1 Internet penetration in Asia**

	1995	2002
Australia *	3.5	46.0
Bangladesh	0	0.1
Bhutan	0	0.1
Brunei	1.03	9.9

<sup>20</sup> S. Chuang (2000). Untapped Asian Market Offers Huge Potential – E-Commerce. *SCMP*, 13 June.

<sup>21</sup> N. Squires & S. Luk (2002). Fraud taints one in 10 Asia deals. *SCMP*, 23 January.

<sup>22</sup> Chuang, Untapped Asian Market; but note that Broadband access also differs with Hong Kong at 77% of Internet users compared to 26% of Japanese and 9% of Australian users.

<sup>23</sup> China Internet Network Information Centre (CNNIC), <http://www.cnnic.net.cn/evolution.shtml>, and the most recent details of the 14<sup>th</sup> Statistical Report on Internet Development in China, 20 July 2004 can be found in English at <http://www.cnnic.net.cn/en/index/00/02/index.htm> visited 6 September 2004.

<sup>24</sup> D. Nairne (2002). China to have most Internet users in 4 years. *SCMP*, 23 April.

<sup>25</sup> *Ibid.*, note 22.

<sup>26</sup> See Hao & Chow, Factors affecting Internet development; and Region in the grips of Internet explosion. *SCMP*, 8 July.

Cambodia	0	0.1
China	0	3.5
Hong Kong	3.28	64.1
India	0.03	0.7
Indonesia	0.03	1.8
Japan	1.59	48.0
Kazakhstan	0.01	0.7
Korea Sth	0.81	52.7
Laos	0	0.2
Macau	0.28	23.0
Malaysia	0.2	24.4
Maldives	0	3.6
Mongolia	0.01	1.6
Myanmar	0	0
Nepal	0	0.2
Pakistan	0	0.3
Philippines	0.03	2.5
Singapore	3.38	55.6
Sri Lanka	0.006	0.8
Taiwan	1.17	49.8
Tajikistan	N/A	0.1
Thailand	0.9	5.7
Turkmenistan	N/A	0.1
Uzbekistan	N/A	0.6
Vietnam	0	0.5

-----  
Source: cited in Hao & Chow; and <[www.InternetWorldStats.com](http://www.InternetWorldStats.com)?; \* Australian Bureau of Statistics (2003)

In the end it is more likely to be the urban/rural divide that will determine Internet access in Asia. Malicious and exploit code are significant global problems and now appear to be generated from within the region as much as from outside.<sup>27</sup>

<sup>27</sup> According to the US security firm Riptech 2002, hacker attacks on corporate computer networks continue to increase. Forty per cent focused on specific targets, and financial services and power and energy companies bore more than twice the number of any other sector, indicating that hackers are now focusing on crucial systems. The report found that the largest number of attacks originated in the United States (30%), followed by South Korea (9%), China (8%) and France (4.5%); see D. Willis, 'United States leads as source of virus invasions', *SCMP*, 11 February 2003. In Hong Kong alone the Computer Emergency Response Team (CERT) received 1500 reported incidents from 11 to 20 August 2003 as a result of Blaster B and So Big F. A Hong Kong Productivity Council 2000 survey revealed that one in three companies in Hong Kong had detected breaches of their security system in the previous 12 months; M. Carlson (2000). Firms plagued by computer viruses. *SCMP*, 12 July.

## [A] Content crime means different things

This paper briefly addresses the problem of ‘content’ crime in cyberspace by looking at both cases and the development of countermeasures within the Asian region. The focus, however, is largely confined to North Asia because this is in part the most advanced IT jurisdiction: South Korea, Japan and Hong Kong SAR have developed some measures to address spamming, pornography (especially child pornography), illegal gaming and hate or racist content on the Internet. The role of ‘Internet content’ policing is also briefly discussed in respect to PR China and Saudi Arabia, where vigorous efforts have been made to broadly control news or religion-related content that is seen as contrary to state interests. These forms of ‘nanny state’ censorship are not all based on filtering or blocking but often rely on proactive strategies such as the promotion of e-governance and services. For example, in China the Internet and ICT is encouraged, so self-censorship is promoted and control by the bureaucracy is often fragmented; in Cuba, on the other hand, access itself is strictly limited.<sup>28</sup>

One current example from PR China may suffice. The Falun Gong is a spiritual movement based on the notion of the natural power of *chi* or *qigong* or life force, and its adherents claim extraordinary benefits in the various meditation and physical exercises it promotes.<sup>29</sup> The Chinese authorities, after appearing to support these ‘physical health’ movements, now regard this movement and other *qigong* (e.g. *Zhong Gong*) as promoting superstition and feudalist beliefs contrary to the PR China constitution and have vigorously suppressed Falun Gong associations and have blocked Falun Gong websites and monitored bulletin boards and chat rooms, including those from abroad. The government sees *qigong* as ‘spreading fallacies, hoodwinking people, inciting and creating disturbances and jeopardizing social stability’ and promoting ‘superstition and malicious fallacies to deceive people, resulting in the deaths of many practitioners’.<sup>30</sup> A *People’s Daily* editorial in July 1999 urged that ‘Party members, government officials, and the people as a whole should understand that this is a serious ideological and political struggle which has bearing on the fundamental beliefs of Party members, on the basic ideological foundation for the Chinese people’s cause and unity, and

---

<sup>28</sup> See Kalathil & Boas, ‘The Internet and state control.

<sup>29</sup> Falun Gong was established in the People’s Republic of China (PRC) in 1992 as a healthy, spiritual and moral exercise program by Li Honzhzhi, but was banned as a political-cult movement in 1999. On 25 April 1999 an estimated 10,000 Falun Gong staged a peaceful demonstration outside the Chinese Communist Party (CCP) headquarters in Beijing to demand official recognition and this appears to have triggered the official ban.

<sup>30</sup> See Kalathil & Boas, ‘The Internet and state control, and K.C. Wong, 2004, *The Criminalization of Falun Gong in China: A Battle for the Hearts and Minds of the People*, unpublished paper – with permission of the author.

on the future of the Party and state'.<sup>31</sup> It could be argued that by applying both reactive proactive forms of Internet censorship, China has been successful in both suppressing *qigong* (Internet) activism and blunting the potential criticisms of its actions.

The notion of 'content' crime in cyber-space reflects more mundane concerns about the medium of the Internet as a vehicle for transmitting and promoting undesirable, amoral or harmful values and behaviour. In addition, the notion that a mere image or text or website can be harmful and therefore the necessary subject of criminalisation challenges liberal traditions of free speech. Nevertheless, the making of certain images sometimes violates the human rights of those involved (as in the case of child or sadistic pornography) and some texts inflame racial, sacred or national hatred, causing loss of life and property in too many incidents. Indeed manipulation of information without any of these 'classic' forms can cause harm that no society can tolerate, as in the example cited below of the HK false 'quarantine crisis' during the SARS outbreak in southern China in 2003.

Individuals can use computers to create social unrest and in Hong Kong a 14-year-old boy was arrested for creating a false website, purportedly authorised by a well-regarded local newspaper. He posted on that website false information concerning the SARS epidemic, stating that Hong Kong would be declared a closed port. This caused widespread panic in the Hong Kong community. One consequence was panic over the quarantine closure, resulting in besieged supermarkets. Calm was only restored some hours later when the government issued repeated public announcements denying the rumour. The boy was arrested and charges were laid after investigators traced the origin of the false site to his computer. He was placed under social welfare care for 12 months (*HKSAR v Sum Cheuk Wa*, FLS 700017/2003). A similar case occurred in Beijing in June 2003. A resident was sentenced to three years for publishing false articles on various websites about the SARS virus. This caused people to stockpile goods and the Chinese papers reported that 'a horrible atmosphere was created and social order was disrupted'.<sup>32</sup>

---

<sup>31</sup> See Senior CPC Official on Falun Gong Prohibition. *People's Daily Online*, 24 July 1999. Falun Gong was banned under the 'Regulations on Registering and Managing Mass Organizations', which require that mass organizations be registered, abide by China's constitution, laws, regulations and policies, and should not violate the fundamental principles of the constitution or jeopardise the interests of the nation and people or of other organisations. It was the position of the PRC government that Falun Dafa Research Society and the Falun Gong had not been registered, and was, therefore, illegal. See Chinese Official Says Falun Gong Ban Follows Chinese Law. *People's Daily Online*, 24 July 1999.

<sup>32</sup> A man was sentenced to 3 years' imprisonment for dissemination of false information on the Internet. *Metro News*, 12 June 2003; see also the case of a young man was convicted in Hong Kong in 2002 and sentenced to 12 months' imprisonment as a result of his cyber-stalking activities. He had accessed victims' computers and sent them e-mails

With the exception of child pornography and the promotion of sex tourism, little consensus is apparent within the Asian region about what might constitute ‘content’ crimes, and in general notions of obscenity and pornography/erotica widely vary across the region. Erotic materials, sometimes blatantly sadistic, available on Japanese and to a lesser degree on Chinese, Taiwan and Hong Kong websites would clearly offend many other jurisdictions but present classic dilemmas about what is obscene or offensive. However, there are simply no reliable estimates of the number of websites or audiences engaged in pornography and as one sceptic noted, ‘they exaggerate everything, especially the size’.<sup>33</sup> Nor is it likely that the industry that purveys such erotica will develop codes of practice that are accepted throughout the region, especially when many Islamic jurisdictions have a ‘zero tolerance’ approach to all kinds of nudity.

Hong Kong’s approach is ‘minimalist and facilitative’.<sup>34</sup> ‘Minimalist’ here means that new legislation will not be introduced if existing laws are adequate to cover activities in the cyber environment. ‘Facilitative’ stresses the importance of partnerships between the Hong Kong Government, the industry, academia and the people to promote benevolent Internet use. Following the passage of the relevant ‘Prevention of Child Pornography Ordinance’ in December 2003, the Hong Kong police in an intelligence-led operation in March 2004 arrested 18 offenders engaged in the downloading and possession of child pornography.

When ‘child pornography’ (*ertong seqing*) was entered into the search engines of Sina.com.cn, Baidu.com, and Google.com.hk, all the results, bar one, cover the crackdown on child pornography in other countries. The only article to refer briefly to such sites in China noted that seven websites ‘publicly selling’ child pornography products had been identified by concerned citizens. The report found that the ‘special section on little girls’ was the best ‘selling point’ of those websites which ‘highly recommend’ hundreds of obscene photos including those of girls as young as 5 or 6 years being raped.<sup>35</sup> The office of ‘sweeping porn and smashing illegal products’ (*sao huang da fei*) was recently established under the auspices of 17 government agencies, including the Chinese

---

threatening them, in some cases with rape, and accompanying the messages with lewd pictures (*HKSAR v Ko Kam-fai*, CACC 82 of 2001).

<sup>33</sup> Cited at [www.caslon.com.au/xcontentprofile2.htm](http://www.caslon.com.au/xcontentprofile2.htm); the same site notes that the only barriers to entry into the cyber-porn market are ‘a sense of embarrassment and the lack of a good lawyer’.

<sup>34</sup> E. Leung (2003). More measures set to fight cyber crime, viewed 10 October 2003, <<http://www.news.gov.hk/en/category/ontherecord/030926/html/030926en11002.htm>>.

<sup>35</sup> See <[http://www.infosec.org.cn/news/news\\_detail.php?mID=1540](http://www.infosec.org.cn/news/news_detail.php?mID=1540)> visited 9 September; translated by Lena Zhong.

Communist Party Propaganda Department, Ministry of Public Security, Ministry of Information Industry and Ministry of Education (see <<http://www.shdf.gov.cn/>>), in order to counter the rapid growth of porn products and pirated products; it encourages the public to report to its 24-hour hotline about porn sites or illegal products in circulation. On 16 July 2004, a national campaign to crack down on porn websites began and within ten days about 700 porn websites were shut down.<sup>36</sup> Despite the detailed coverage of the crackdown on child porn in other countries, the focus of government and media attentions has been on protecting youth from 'pornographic pollution' rather than on the arrest of the manufacturers and purveyors of child pornography in China.

There is, however, growing concern about the role of the Internet in promoting racial/ethnic hatred in many Asian countries, particularly in nations that have large religious minorities such as the Philippines and Thailand with large Muslim populations and Indonesia with a significant Christian minority. In all these jurisdictions national laws prohibit racial or religious vilification and have moved to suppress these forms of expression on the Internet and in the print media. Inflammatory allegations and images of rape and mayhem against Chinese Indonesians during the 2000 riots were widely disseminated via Chinese chat rooms and in turn caused anti-Indonesia sentiment to run high throughout urban China. During the Cambodian elections in 2003 and 1998, opposition parties advocated harsh measures against Vietnamese residents, causing considerable property damage and injury among that minority. A script by a Thai TV actress that claimed Angkor Wat as a Thai site in 2002 was widely disseminated by Cambodian print and radio after appearing on an Internet website and chat rooms; the result was the destruction of the Thai Embassy and an estimated \$US20 million damage bill to Thai businesses in Cambodia before order was restored. Images of the Thai King's portrait being trampled on by Cambodian rioters were shown repeatedly on Thai television, in turn causing expressions of anti-Cambodian feeling on the streets of Bangkok.<sup>37</sup> The very volatility of these behaviours and their vulnerability to misinformation and racial/ethnic vilification renders the control of inflammatory content a matter of serious concern to law enforcement agencies tasked with public order, throughout the region.

#### **[A] Accessing content for investigative purposes**

---

<sup>36</sup> See <<http://news.sohu.com/20040727/n221227710.shtml>> visited 9 September; translated by Lena Zhong.

<sup>37</sup> *Phnom Penh Post*, 13, July 2002.

Content is the data contained in a communication, and access is generally more tightly controlled than access to traffic data. In many cases laws permit access to content processed by ISPs. But if the subject is using a computer within a corporate network, or where data is transmitted in encrypted form over a virtual private network, actual content may not be available from ISPs. In these cases legislation may need to allow the preservation of, and access to, content on those networks. Again, legislation should balance the needs of law enforcement with the burden on parties in collecting and storing the data. Also geo-location approaches (e.g. Quova, NetGeo, javanetlocator) that matches a user's Internet address with a place is a developing (if fraught) technology that has the potential to make the Internet less borderless than supposed and already has a role in identifying content crimes and fraud.<sup>38</sup>

ISPs and system administrators are often confused by seemingly conflicting requirements to collect, store and allow access to information on the one hand and requirements to protect privacy and ensure secrecy of communications and information on the other. The situation is further complicated where multiple law enforcement agencies are involved or where ISPs operate in multiple jurisdictions. There is a need for governments to provide clear guidance to ISPs and system administrators on their obligations and the processes involved in complying with lawful requests for collection and storage of information and access to it. A separate question is the need for governments to recognise legitimate security activities when framing legislation. This particularly concerns tools that can be legitimately used for security testing but illegitimately to access or damage computer systems. Legislation will need to distinguish legitimate from illegitimate use.<sup>39</sup> Identifying and prosecuting harmful content sites will not be easy and borrowing some of the techniques and approaches of the anti-counterfeit and IP protection may be helpful.<sup>40</sup>

---

<sup>38</sup> See generally B. Schneier (2000). *Secrets and Lies: Digital Security in a Networked World*, New York: Wiley.

<sup>39</sup> S. Orlowski. (2004). APEC Activities to Address Cybercrime Through Public/Private Cooperation. *Proceedings of the 2nd Asia Cyber crime Conference*. University of Hong Kong.

<sup>40</sup> The Business Software Alliance (BSA) 2001 Piracy Report found that the overall piracy rate in the Asia-Pacific region had increased after declining steadily between 1994 and 1999. The regional revenue loss to software corporations was estimated to be US\$4.7 billion in 2001. The highest piracy rates in Asia and the world were Vietnam 94% and China 92%. The BSA estimates that stolen software cost the industry US\$13.1 billion in 2002 (see P. Grabosky & R. Smith (2001). *Crime in the Digital Age*. Cambridge University Press, p. 7). In the Asia-Pacific region alone, the estimated theft in software copyright theft was US\$5.5 billion. It has been suggested that one in three computer software programs sold worldwide is a counterfeit. In 2002 the sale of pirated CDs rose 14% to 1.1 billion – more than double the previous three years. It cost the industry US\$4.6 billion according to the International Federation of Phonographic Industry; B. Warner, 'Sales of Pirated CDs top 1 billion 2002', *Bangkok Post*, 11 July 2003.

Interventions such as Microsoft’s bounty on virus software writers, IFPI’s general focus on deterrence to frighten the average law-abiding ‘music pirate’ may not be applicable to suppressing content crime. Although such an emphasis on deterrence by paying as much attention to small and big players may offer some relief, it is unlikely to deter ardent racists. However, BSA’s<sup>41</sup> deployment of automated ‘web-crawling’ software to identify bogus or illegal websites is a yet unproved measure, despite impressive efforts shown in Table 2. Cyber-patrols can be automated but nevertheless still require human intelligence to sort through ‘hits’ identified via key word and other search techniques. Apart from the vastness of the task, Chinese script poses technical problems for these methods. It is acknowledged that ‘web-crawler’ technology is imperfect and that ‘take-down’ notices do not end infringing websites but often displace them to other jurisdictions or lead to their reinvention in less detectable form.

**Table 2: BSA Automated ‘web-crawler’ activity, January–September 2003**

Region	Infringing sites	‘Take-down’ notices
Asia	38,907	15,242
Europe	483,659	17,739
Latin America	83,524	17,650
North America	634,267	87,723
All	1,240,357	138,354

Table 2 suggests that most of the identified activity takes place in Europe (39%) and North America (51%), but effective ‘take-down’ is very low in Europe (3.7%) and North America (13.8%) compared to Asia (39.2%) and Latin America (21.1%). It is most likely that the relatively low identification of infringing sites in Asia is a function of the present inefficiency and special problems faced by search engines encountering Chinese (either traditional or simplified) and other non-European languages. Indeed the need for such multilingual search engines is a major research priority and may prove highly useful in increasing the risks of interdiction for cyber-criminals. As criminologists would recognise, data of the kind reported in Table 2 is more likely to reflect the

<sup>41</sup> The BSA was founded in 1988 with the purpose of protecting the copyright of the computer software industry and now operates in 68 countries.

activity of the enforcers than of the criminals, and basic research on the prevalence, nature and gravity of cyber-crime is essential. At present too little is known about the patterns of criminality or victimisation and this reflects the low priority given to fundamental criminological research in preference for research on technological fixes.

Within Asia, the Japanese National Police Agency (NPA) has established an international investigative cooperation framework, the Cyber-crime Technology Information Network System (CTINS) and has been promoting measures in accord with the Council of Europe's Convention on Cyber-crime, which the Government of Japan has now adopted.<sup>42</sup> The focus to date has been on traditional theft offences and child pornography, while little effort has been made to address the civic need to suppress 'hate speech'. However, prefectural police hold regular Connection Conferences with ISPs which include training and information-sharing, especially with regard to countermeasures against cyber-crime, such as exclusion of illegal and harmful information on the Internet. Defamation offences have been pursued against individuals and web-page creators. They also play an active part in public education about information security, cooperating with consumer unions and educational institutions so as to protect citizens from the danger and damage of cyber-crime. Moreover, the police conduct seminars about information security for the staff of educational institutions, public institutions and private enterprises and exchange opinions with them in order to improve information security consciousness.<sup>43</sup>

### **[A] Unsolicited Commercial Email (UCE) and Spam**

Another menace, with equally insidious effects, is the rapid spread of 'spamming'. This is one vector for the spread of 'content' crime, often helped along by the availability of ubiquitous CDs offering 300 million addresses for US\$99. Organisations such as 'SpamCop' and 'StopSpam' actively target irresponsible spammers and their ISPs, while more effective filtering can blunt the impact but rely on the user being an active player. In Korea pioneering responses to the ubiquitous menace of 'spam' have been developed by the Korean Information Security Agency (KISA).<sup>44</sup> In the Korean

---

<sup>42</sup> T. Sato (2004). Cyber crime countermeasures in Japan. *Proceedings of the 2nd Asia Cyber crime Conference*. University of Hong Kong.

<sup>43</sup> Ibid.

<sup>44</sup> A US federal law is pending on an anti-spam measure that will supersede 37 state laws and increase penalties and measures against illegal spam. An Australian Spam Bill was also introduced in 2003: see <<http://www.aph.gov.au/library/pubs/bd/2003-04/04bd045.htm>>. A number of proposals have suggested the establishment of a dot.XXX cite for Adult pornography.

example, efforts to criminalise this conduct and to stress the critical role of consumer awareness have proved somewhat effective, but extra-jurisdictional ‘spammers’ still operated with relative impunity. KISA provided data that estimated that on average 41 ‘spam’ mails were received per person per day in Korea in July 2003; this is down from about 50, but unless spamming is addressed e-mail systems are likely to be flooded to extinction.<sup>45</sup> KISA noted that many ‘relay servers’ were sourced from schools and that improving information security in that sector along with requiring ISPs to register bulk mailers may stem the flood of unsolicited commercial e-mail. According to a KISA survey, 56% of ‘spam’ involved sexually explicit material, 19% other illegal products, 14% fraud-style e-mails, and 11% other forms of advertising.<sup>46</sup>

A recent Australian Government report found that computers were being used in spam e-mails touting black market drugs, celebrity porn, bogus prizes and Nigerian money laundering frauds. The findings in the Australian report are also reflected in the result of a recent (May 2003) US Federal Trade Commission Study, which found that two-thirds of spam contains one or more fraudulent elements. Further, about 18% of all spam studied by the Federal Trade Commission (FTC) involved pornography or other sexual products.<sup>47</sup> In Hong Kong 10–30% of the e-mails received by local users were spam according to the Chamber of the Hong Kong Internet Service Providers Association, and the amount of spam mail originating in China is increasing with the growing population of Internet users in China.<sup>48</sup> An anti-spam summit held in Beijing on 24 April 2004 revealed that on average every Internet customer in China received 19.3 spam e-mails every week, a one-third rise compared with the previous year. Since August 2003, the anti-spam section of the Internet Society of China has published three ‘blacklists’ of spam URLs (Chinese and overseas) and claims that China will become the largest anti-spam market worth 10 billion Chinese dollars.<sup>49</sup> According to a UK anti-spam organisation. ‘Spamhaus Project’, 80% of US spammers have moved their servers to the Chinese market, choosing Liaoning as the base.<sup>50</sup> According to US anti-spam

---

<sup>45</sup> KISA cited data that estimated spam comprised about 50% of emails but predicted by 2005 80% of emails would be spam. Message Labs, an email security system provider, estimates that spam accounted for one in every 2.5 emails in 2003 compared to one in 11 in 2002 (A.M. Squeo. US House Advances Spam Bill. *Asian Wall Street Journal*, 10 December 2003).

<sup>46</sup> Cited in R. Broadhurst (2004). Rapporteur’s Report. *Proceedings of the 2nd Asia Cyber crime Conference*. University of Hong Kong.

<sup>47</sup> Agencies in Washington (2003). Pressure but for anti spam laws. *SCMP*, 6 May.

<sup>48</sup> S. Luk (2002). HK ignorance spawns spam. *SCMP*, 1 October.

<sup>49</sup> See *IT Times Weekly*, 10 June 2004. In 2003 spamming was estimated to be worth 4.8 billion Chinese dollars; see <Phoenix.com>, 8 December 2003.

<sup>50</sup> Spamhaus traced two ‘mystical messages’ sent by the US ‘spam king’ Alan Ralsky to Fushun and Dandong in Liaoning province; Lei Zhonghui, ‘21 Century Economic Report’, 26 May 2004.

company 'Commtouch', which followed through 300,000 spam messages in 2003, 71% used servers in China. However, rather than suggesting that the senders of spam messages are Chinese Internet users, the company found the spammers were more likely from the United States or Europe.<sup>51</sup>

A good example of the use of computers in committing fraud through spamming was seen in a case uncovered in the United States in 2002, which involved fraudulent e-mails. The fraudsters had spammed computers promising the recipients free Sony play-station games. Those who responded were directed to a bogus website that instructed them to download a program which allowed them to collect the prize. The program in fact connected them to a pornographic website which charged them US\$3.99 per minute. The product delivered was offensive to adults and totally inappropriate for children. The fraudsters took in US\$11 million. The website was shut down and the FTC sought to recover the money obtained.<sup>52</sup> The spamming of '419' advanced fee fraud letters is also a widespread phenomenon but has not led to any arrests in Hong Kong. E-mail header analysis suggested that the e-mails were mostly send via an open server relay located in the US, India or Mainland China. The growing use of worm-based intrusions to spread spam, especially dubious or illegal products, has also been noted but as yet no arrests for spam/worm authors has been reported in the region. Spammed e-mails of bogus e-Banking websites of famous banks or financial institutes, (e.g. HSBC, Standard Chartered, Citibank or their hyperlinks) has also emerged in Hong Kong as an efficient means of locating victims. The unsuspecting (naive) victim is asked to submit their e-Banking login ID and password for verification or security checking.<sup>53</sup>

Illegal online gambling is also another new crime to emerge in China, but early cases simply used the Internet as a means to advertise activities rather than as an interactive gambling site. However, increased sophistication has been noted, with a recent trans-national illegal online gambling operation detected by the police in July 2004 and the arrest of 47 in Yiwu, Zhejiang Province, was connected with a casino in Burma. The police also found similar organisations in neighbouring counties and cities within Zhejiang Province and Shanghai.<sup>54</sup> Beijing Customs have seized thousands of online gambling CDs since November 2003 following the 15 March 2003 seizure of 618 online gambling CDs sent from Switzerland. The recipients of were located in all 20 provinces of China

---

<sup>51</sup> See <<http://www.mailer.com.cn/article/articleprint/1602/-1/151>>, visited 9 September 2004.

<sup>52</sup> Reuters Washington, 'Fraudulent e-mail sent to Playstation witness to porn site', *SCMP*, 26 April 2002.

<sup>53</sup> Personal communication, Mr Frank Law, Technology Crime Division, HKP.

<sup>54</sup> *Peoples' Net*, 12 July 2004.

and it is suggested that online gambling organisations have begun to infiltrate China.<sup>55</sup> Cases of this kind are relatively new in China and the local newspaper reports often headline them as the first in a province or city. An Internet gambling website was found hosted by a Hong Kong web-server. No person was arrested but the website was removed after advice and the ISP was warned of the possible violation of laws.

Another problem arises with popular web-services such as UK site 'Sharpmail' that posted bogus e-mails allowing the user to send messages from any address and re-routing the reply to the user's personal mail. Although yet to be mimicked in Asia, this service has proved a bonus for pranksters, who have used it to send bogus messages to colleagues apparently from the bosses' address (you're fired!) or the local police (you're needed for questioning).<sup>56</sup>

#### **[A] Public confidence**

Internet content liability and regulation issues are being addressed in the United States and Europe through a mix of direct legislation, industry self-regulation and third-party interventions.<sup>57</sup> It is likely that governments outside the EU will begin drawing up privacy laws in the next three to five years. Given estimates that the e-business market in the Asia-Pacific will reach US\$910 billion by 2004,<sup>58</sup> security of transactions must be addressed. Recent surveys in Japan and South Korea suggest that the degree of distrust of the way Asian websites handle privacy is greater than the distrust in the United States and Europe. Current figures released for the Asian region suggest that as many as one in ten online consumer transactions may involve fraud, with similar rates likely for business and government.<sup>59</sup> As a result, the Asia Pacific Internet Association commissioned a study to explore the viability of self-regulation, and to outline a model code as well as a possible mechanism for self-regulation. Key proposals included the voluntary labelling of websites under the Internet Content

---

<sup>55</sup> *China News Weekly*, 29 March 2004

<sup>56</sup> Agencies Press (2004). Bogus E-mails Worry Police. *SCMP*, 21 August.

<sup>57</sup> As an example, the US directs the Internet Fraud Complaint Centre, while the UK is setting up the Centre for Cybercrime Complaints. 'Calls for cybercrime database', *BBC news online*, 29 August 2001, <[http://news.bbc.co.uk/hi/english/business/newsid\\_1514000/1514215.stm](http://news.bbc.co.uk/hi/english/business/newsid_1514000/1514215.stm)>.

<sup>58</sup> Gartner Group survey, cited in M. Bray, 'Fraud hits one in ten Asian Internet deals', <*CNN.com*>, 20 March 2002; <<http://www.cnn.com/2002/BUSINESS/asia/03/20/asia.net/>>.

<sup>59</sup> Australian Institute of Criminology, 'E-commerce fraud on the internet rarely reported', Media Release, 17 January 2002; <<http://www.aic.gov.au/media/2002/20020117.html?>>.

Rating Association rating scheme.<sup>60</sup> This would protect users and provide guidelines for business in the event of security breaches like fraud or child pornography or hate speech.

### [A] Content censorship<sup>61</sup>

In April 1999 a Singapore law student complained after an anti-intrusion program she installed indicated that someone with an account in the Home Affairs Ministry had hacked into her computer. It was revealed that the internal-security agency had secretly scanned 200,000 computers to trace a virus. SingNet, the Internet service provider, acknowledged that it asked the Ministry's IT security unit to scan its customers' PCs for viruses without their consent. SingNet is owned by Singapore Telecom, which is in turn 80% owned by the government. The request to conduct the scan was reportedly made after the arrest of two youths who had hacked into 17 SingNet accounts.<sup>62</sup> SingNet claimed the scanning did not 'enter' any PCs or compromise any personal data and that it found 900 PCs infected with Trojan horse viruses that allowed hackers to enter computers via the Internet.<sup>63</sup> Nevertheless, public outcry over the incident eventually led to an official apology from SingNet

A 2001 Council of Minister's Resolution prohibits users within the Kingdom of Saudi Arabia from publishing or accessing certain content on the Internet. Web traffic is apparently forwarded through a central array of proxy servers in the government's Internet Services Unit. A Harvard study evaluated the scope and effectiveness of these filtering mechanisms and connections were made to the Internet through proxy servers in Saudi Arabia. The survey explored the effectiveness of the filtering mechanisms as well as the nature of the blocked pages. Of approximately 60,000 web-pages tested, the authors tracked 2038 blocked pages. These pages contained information about religion, health, education, reference, humour and entertainment.<sup>64</sup> The authors concluded that 'the Saudi government maintains an active interest in filtering non-sexually explicit Web content ... substantial

---

<sup>60</sup> H.A. Peng [n.d] Code of Practice For Internet Content Self-Regulation. *Report to the Asia and Pacific Internet Association*. Nanyang Technological University, Singapore; <<http://www.apia.org/sreexecutivesummary.htm>>.

<sup>61</sup> I am greatly indebted to the discussion on this topic offered by Shannon, J. & N. Thomas, 2004, 'Human Security and Cyber-Security: Operationalising a Policy Framework', in R. Broadhurst & P. Grabosky (Eds.). *Cyber-Crime: The Challenge in Asia*. University of Hong Kong Press.

<sup>62</sup> Singapore Government Scans 200,000 Users Computers. *Asian Wall Street Journal*, 6 May 1999.

<sup>63</sup> How personal are personal computers? *Far Eastern Economic Review*, 20 May 1999; <[http://www.feer.com/Restricted/99may\\_20/tech.html](http://www.feer.com/Restricted/99may_20/tech.html)>.

<sup>64</sup> J. Zittrain & B. Edelman [date?]. Documentation of Internet Filtering in Saudi Arabia. Center for Internet and Society, Harvard Law School; <<http://cyber.law.harvard.edu/filtering/saudi-arabia>>.

amounts of non-sexually explicit Web content is in fact effectively inaccessible to most Saudi Arabians; and ... much of this content consists of sites that are popular elsewhere in the world.’<sup>65</sup>

The most frequent form of content censorship occurs when the government blocks or filters a website. Approximately 59 nation-states restrict public access to information by blocking Internet sites.<sup>66</sup> The Saudi Arabia study showed that the censored websites included those relating to women’s rights, health issues and sexuality. The government cites the Koran, describing its filtering role as ‘preserving our Islamic values, filtering the Internet content to prevent the materials that contradict with our beliefs or may influence our culture’.<sup>67</sup> In China, Internet filtering focuses on news sites and political content critical of the Party, reflecting concerns over political subversion, ‘splittism’ and Taiwanese independence.<sup>68</sup> Recently there have been further attempts at ‘cleaning’ media content in print, TV and the Internet, with standards of dress, content and language subject to ‘decency’ tests. China has also blocked access to the search engines Google and Alta Vista, and news sites such as the BBC, SCMP and Amnesty International.<sup>69</sup> It has also concluded agreements with search engines such as Yahoo! that prevent the posting of any information offensive to the Chinese Government.<sup>70</sup>

In comparing the China and Saudi Arabia examples, where both countries censor materials deemed harmful, in the case of Saudi Arabia the emphasis is on the state’s role in aiding the security of the individual, whereas in China “...the emphasis is on the individual’s role in the security of the state”<sup>71</sup>, as part of the proactive strategy of encouraging self-censorship. This difference according to Shannon & Thomas is shown in the way sites are filtered by the two governments: “Attempting to access a restricted site in Saudi Arabia results in an ‘access denied’ message appearing on screen, alongside information concerning the blocking policy and a request form for the government to reconsider its block on the site. Attempting to access a restricted site in China, however, results in a ‘host not found’ message, leaving the user uncertain as to the cause of failure for the connection. Key word filtering and the discarding of e-mails containing key terms is also used by the Chinese

---

<sup>65</sup> Ibid, cited in Shannon & Thomas (2004:339).

<sup>66</sup> Reporters Sans Frontières (2001). Enemies of the Internet. <<http://www.rsf.org/ennemis.php3>>.

<sup>67</sup> Cited in Zittrain & Edelman. Documentation of Internet filtering in Saudi Arabia.

<sup>68</sup> N. Shachtman (2002). Why countries make sites unseen. *Wired*, 18 July; <<http://www.wired.com/news/politics/0,1283,53933-2,00.html>>.

<sup>69</sup> M. Musgrove (2002). In China, some regain access to Google Site’, *Washington Post*, 13 September; <[http://www.washingtonpost.com/wp-adv/advertisers/popunders/verisign\\_oct02.html](http://www.washingtonpost.com/wp-adv/advertisers/popunders/verisign_oct02.html)>.

<sup>70</sup> D. Lee, ‘Multinationals making a mint from China’s Great Firewall’, *SCMP*, 2 October 2002.

<sup>71</sup> Shannon & Thomas (2004:340)

authorities, but without informing its citizens as to exactly what the terms are and what words are in the lists”<sup>72</sup>. Thus in Saudi Arabia a user knows what has happened and has a limited opportunity for corrective action, but in China the user is unable to take action as the actual cause of the ‘host not found’ message is unclear.

As cultural values differ greatly within Asia, regional agreement on content and censorship has led to acknowledgment of these differences. The International Telecommunications Union for Asia and the Pacific argued that ‘the issue is not regulating Internet content per se, but protecting vulnerable groups with technical apparatus or regulatory measures’.<sup>73</sup> In China, violations of its regulations can lead to the death penalty or imprisonment for relatively minor actions.<sup>74</sup> In mid-October 2003, Luo Yongzhong was imprisoned for three years by the Changchun intermediate court in Jilin Province for eight anti-government postings in chatrooms.<sup>75</sup> Since the introduction of the Internet in 1997, Vietnamese authorities have strictly controlled access to certain sites, following a regulatory system similar to that used in China.<sup>76</sup> In another case in late 2003, Vietnamese journalist and cyber-dissident Nguyen Vu Binh was sentenced to seven years’ jail for espionage after criticising Vietnam–China border accords, which were then e-mailed to other domestic groups as well as to lobby groups overseas.<sup>77</sup> In Myanmar, where public access is denied, unauthorised use of a computer or a modem earns users up to 15 years in jail.<sup>78</sup>

## **[A] Prevalence of recorded Internet crime**

For those jurisdictions which have in place substantive laws that criminalise various aspects of computer crime, statistics on known offences are consequently available. However, few law

---

<sup>72</sup> Ibid

<sup>73</sup> The International Telecommunications Union Regional Preparatory Meeting, Asia and the Pacific, Policy and Regulation, Issue Paper for the World Telecommunication Development Conference, 2002; cited in Shannon & Thomas, Human Security and Cyber-Security.

<sup>74</sup> For discussion of state regulations regarding the Internet see Human Rights Watch. [n.d.] Freedom of Expression and the Internet in China: A Human Rights Watch Backgrounder, <[www.hrw.org/backgrounder/asia/china-bck-0701.htm](http://www.hrw.org/backgrounder/asia/china-bck-0701.htm)>. Two Chinese cyber-activists, Hu Mingjun and Wang Sen, were sentenced to death for spreading anti-socialist writings. Two others, Ouyang Yi and Li Zhi, are awaiting sentencing and trial (respectively) for similar anti-state cyber-behaviour that also carries the death penalty.

<sup>75</sup> China sentences another dissident for posting views on Internet. *Agence France Presse*, 22 October 2003.

<sup>76</sup> Reporters Sans Frontières (2002). Le Gouvernement Vietnamien Imite le Modèle Chinois de Contrôle de l’Internet. 7 August; <[http://www.rsf.fr/article.php3?id\\_article=3307](http://www.rsf.fr/article.php3?id_article=3307)>.

<sup>77</sup> S. Collinson (2003). US gives Vietnam a tongue lashing after cyber dissident jailed, *Agence France Presse*, 31 December; and Vietnam: Cyber dissident jailed for seven years. *Global News Wire*. 5 January 2004.

<sup>78</sup> N. Shachtman (2002). Why Countries Make Sites Unseen. <*Wired.com*>, 18 July 2002; <<http://www.wired.com/news/politics/0,1283,53933,00.html>>.

enforcement agencies distinguish data based on the precise nature of the ‘cyber-crime’. Data for Japan and Hong Kong are briefly discussed and the trends include significant changes in the nature of the offences reported and increases in more serious offences. For example, in Japan arrests for computer-related crimes involving the Internet were 31.7% of 262 arrests in 1997 and 29.9% of 415 arrests in 1998, but by 2002 they accounted for 92.2% of all 1039 computer-related arrests, with a growing trend in fraud-like offences noted. In the case of Japan the majority of Internet-related crimes involved pornographic and associated offences.

**Table 3: Internet and computer crime in Japan**

	2000	2001	2002
<b>Crime against computer/data</b>	<b>44</b>	<b>63</b>	<b>30</b>
Computer fraud	33	48	18
Illegal production/destruction of data	9	11	8
Obstruction of business by destroying computer	2	4	4
<b>Internet crime</b>	<b>484</b>	<b>712</b>	<b>958</b>
Child prostitution	114	117	268
Child pornography	64	128	140
Fraud	53	103	112
Distribution of obscene object	154	103	109
Violation juvenile protection ordinance	25	10	70
Intimidation	18	40	33
Infringement of copyright	29	28	31
Defamation	30	42	27
Others	78	14	168
<b>Unauthorised computer access</b>	<b>31</b>	<b>35</b>	<b>51</b>
<b>Total</b>	<b>559</b>	<b>810</b>	<b>1039</b>

In January 2001, the Government of Japan launched its E-Japan Strategy, which has as its goal making Japan the world’s most advanced IT nation within five years. During 2002, the arrest number for cyber-crimes in Japan reached 1039, the highest so far. Among these, Internet crime increased 35% over the previous year. The number of content crimes made up 46% of reported cases and involved 408 child prostitution and child pornography cases, and 70 cases of violation of the

*Juvenile Protection Ordinance* (see Table 3). Arrests for fraud in online auctions also increased.

Japan has established counselling consultations with victims about cyber-crime and during 2002 this was 19,329, an increase of 12% over the previous year (see Table 4). Of these, the number concerning online auctions was 3978 or 20.5%, consultations about fraud and criminal business on the network was 3193 or 16.5% 1.6 times that of the previous year and defamation cases 13.3% of all victims.<sup>79</sup>

**Table 4: Trends in cyber-crime victim counselling in Japan**

<i>Type of victim</i>	<i>2000</i>	<i>2001</i>	<i>2002</i>
Fraud	1396	1963	3193
Internet auction	1301	2099	3978
Defamation	1884	2267	2566
Unauthorised access/virus	505	1335	1246
Spam mail	1352	2647	2130
Illegal information	2896	3282	2261
Others	1801	3684	3955
<i>Total</i>	<i>11135</i>	<i>17277</i>	<i>19329</i>

Source: NPA

Hong Kong police statistics for reported computer-related offences show rapid increases in hacking and deception offences and significant increases in 2003. ‘Content’ offences, on the other hand, have received serious attention only with the passage of child pornography laws late in 2003 which prohibit the possession and dissemination of child pornography; as yet no specific laws are in place to deal with hate crime. Although intrusion offences are often minor, they are now commonly **seen** in conjunction with deception offences. Intrusion offences are now more likely to be a predicate to more serious offences. Increases in 2003 were also associated with the popularity of online games in Hong Kong.

<sup>79</sup> Details cited in Sato. Cyber crime countermeasures in Japan. An office worker (32) reproduced without permission the map survey software, which was being used in an office, exhibited the software on an FTP site on the Internet, and made it capable of being downloaded by the general public. In September 2002, Miyagi Prefectural Police arrested him for violation of the *Copyright Law*.

## Conclusion

Where data is available that distinguishes content offences, as in the case of Japan, the contribution of ‘content’ crimes is significant, but we know little about the extent and prevalence of even the content offences of greatest concern – child pornography and hate crimes. In respect to risks to children of unsolicited sexual contacts, we also have no clear data for Asia of the kind provided in the United States, where a 2001 study found that one in five of 10–17-year-olds had received such a contact in the preceding year, although 4% received ‘aggressive’ solicitations (off-line contact sought).<sup>80</sup> However, a recently released survey conducted in March–April 2004 by Against Child Abuse of the on-line activities of 1,175 Hong Kong high-school students aged 12–15 showed that 55% of them had made friends with strangers contacted on the Internet. Of these 39.5% went on to meet their on-line contact, 12.3% subsequently dated and 6.9% had sexual contact. A significant proportion (11.6%) suffered financial loss after meeting their on-line acquaintance and 9% were sexually assaulted or harassed<sup>81</sup>. Generally the ‘metrics’ of the prevalence or extent of these content crimes among, for example, the estimated 18 million active but volatile domains (in mid-2000) and 1.4 billion publicly accessible pages are unreliable and few studies are available.<sup>82</sup> Porn industry claims that e-commerce was developed because of the Internet’s advantages in pioneering the selling of Adult content are also highly questionable.<sup>83</sup> However, businesses that provide content filtering software and services (such as online age verification services) are among the most profitable, particularly as these services are promoted as part of an integrated IT management for corporations and institutions.

The cultural and jurisprudential diversity of Asia poses a challenge to the harmonisation of laws aimed at addressing the most serious aspects of hate crime and pornography. The relative effectiveness of many Asian jurisdictions at controlling the use of the Internet through proactive strategies (e.g. notably Singapore) also suggests that the Internet performs just as well as a means of propaganda as it does for putative reformers. This also suggests that relatively effective control of

---

<sup>80</sup> The sample comprised 1501 teenagers who used the net regularly; see D. Finkelhor, K. Mitchell & J. Wolak (2001). Risk factors for and impact of online sexual solicitation. *Journal of the American Medical Association*. Cited at <[www.caslon.com.au/securityguide11.htm](http://www.caslon.com.au/securityguide11.htm)>.

<sup>81</sup> Moy, P. (2004). Teens admit outings, sex with net strangers. *SCMP*, October 4, 2004: C3.

<sup>82</sup> E. O’Neil, B. Lavoie & R. Bennet (2003). Trends in the evolution of the public web, cited in <[www.caslon.com.au/metricsguide1.htm](http://www.caslon.com.au/metricsguide1.htm)>.

<sup>83</sup> See F. Lane (2000). *Obscene Profits: The Entrepreneurs of Pornography in the Cyber Age*. London: Routledge.

'content' crimes is possible and the development of geo-locational technologies may make transnational investigations more feasible. The low IT and Internet penetration in many of the Less Developed Countries of Asia also imply that cyber-policing remains vulnerable to 'weakest link' problems, although access controls may work effectively if the relevant expertise is available. Here the aid efforts of 'liberal' democracies may result in providing capabilities designed to fight cyber-crime that is equally useful in censoring and controlling expression and cherished 'free speech'.

In relation to the 'content crimes' infesting cyberspace, there may be excessive hype over them but it seems increasingly clear that many jurisdictions including many in Asia will have to address the role of the Internet as a vector for hate and child pornography. Many Asian leaders will be less troubled by the curtailment of such individual 'free speech' in the context of their communitarian societies, but unless there is a modicum of agreement about how content crimes are defined, the prospects for a multilateral agreement are slight and are unlikely to be 'smuggled' into nascent consensus on the need to address other cyber-crime such as malicious code and Internet fraud. In the interim, self-help, public opinion and responsible industry guidelines may enable such activities to be curtailed.