8. Dumbing down democracy: Trends in internet regulation, surveillance and control in Asia

ABSTRACT

This article argues that the trends in state regulation, surveillance and control of the internet in Asia stand to effectively reduce political expression. A variety of international media watch and human rights organisations have noted that since 11 September 2001, a slew of anti-terrorism laws have been adopted in Asia which place greater restrictions on the internet. Laws against online pornography, gambling, hate speech and spam have been revised to cover online political content and mobilisation. Such measures limit and reduce the space cyberactivists have to push the democratic agenda online. These cybersecurity measures, introduced as part of the 'war against terrorism', represent an extension of already draconian regulations in South-East Asian countries.

JAMES GOMEZ
Monash Asia Institute, Monash University

Introduction: Post-September 11 online legislation

THE RELATIONSHIP between the growth of the internet and attempts to control it can reveal a lot about the potential for cyber-democracy. In this regard it is important to note that the terrorist attacks of 11 September 2001 (9-11) have speeded up efforts to control the previously free space provided by the internet. In Asia a slew of anti-terrorism laws has been adopted drawing upon the *UN Resolution 1373*, the *USA Patriot Act* and various European laws.

Reporters Sans Frontieres (RSF) has called 2003 'a black year' for journalists. Asia has been declared the 'world's largest prison for journalists, cyber dissidents and internet-users'. China has the biggest number of internet-users in prison; a total of 48 at 1 January 2004. Nine cyber dissidents are jailed in Vietnam, and according to Reporters Sans Frontiers, the country has set up a computer research department exclusively devoted to creating internet surveillance software (RSF, 6 January 2004).

Reporters Sans Frontieres(RSF) asserts that the internet has suffered 'serious battering' since 9-11 and is 'collateral damage' in the war against terror (RSF, 2002: 1). The threat of 'terrorism' has been used in many countries as a justification for increased security measures, including surveillance, and a reining in of civil liberties such as freedom of expression. Following the Bali bombing in October 2002, for example, the Indonesian Government enacted anti-terrorism regulations, increased police powers and allowed for detention without trial (this had previously been rejected by Parliament).

The Electronic Privacy Information Center (EPIC) and the Privacy International report entitled *Privacy and Human Rights 2003* identified global trends in governmental and legislative surveillance following 9-11. Those were; increased communications surveillance; weakened data protection regimes; increased data sharing; and increased profiling and identification.

RSF, EPIC and Privacy International are in agreement that: 'None of the above trends are necessarily new; the novelty is the speed with which these policies gained acceptance, and in many cases, became law' (EPIC & Privacy International, 2002: 27). The asserted need to track terrorists, whose primary use of the internet appears to be the same as us 'non-terrorists' – for communication and discussion – increased the apparent urgency of cyberspace tracking. Ultimately, according to the RSF, 'the presumed use of the internet by members of the terrorist command to contact each other and prepare the operation handed a victory to advocates of very tough security measures and strict regulation of the internet' (RSF 2, 2002: 4).

While much of the above discussion centres on managing the technology in order to counter terrorist threats, one must also recognise that there are historical tensions between technological development and democratic principles in Asia. Hence, like other past technological innovations such as the radio, television, fax machines and satellite broadcasting, the internet represents a new type of medium that governments, as always, are keen to control.

The popular assertion often made by internet advocates is that content control, a primary characteristic of the traditional state-media relationship, cannot be as successful or far-reaching when applied to the internet. However, this is not the case. In Asia, since 9-11, governments have tabled or passed legislation that will enable them to track and monitor content that is put online (Privacy International, 2003). Governments are giving electronic snooping powers to themselves and their various agencies to spy on others.

These developments raise important questions. Can the public be reasonably sure about the transparency of governments, even democratic ones? How should the rights of the individual be reconciled with the safety of the community? Here it is important to note that important state functions like surveillance are being sub-contracted out to private, commercial firms – in the name of anti-terrorism.

At the international level there were concerns that the first World Summit on the Information Society (WSIS), would prompt some countries to promote restrictions on the internet and other information technologies (Shashi Tharoor, 2003). What emerged was a joint declaration at the December 2003 WSIS in Geneva to affirm commitment to internet freedom (WSIS, 2003). Nevertheless the desire of governments to restrict internet usage continues unabated. Within national territories governments retain the legal and legitimate right to regulate computer-mediated communication.

Within this context I will examine the relationship between new media and democracy in the post-9-11 period. Starting with the early introduction of anti-terrorism legislation, regimes in Asia have sought to control the political content of the internet. Attempted government restrictions are complicated by the fact that internet technology is evolving rapidly. To the extent that such restrictions are successful the internet's democratic potential is weakened. More importantly, cybersecurity measures, introduced as part of the 'war against terrorism', represent an extension of already draconian censorship and surveillance regulations in South-East Asian countries.

Democracy, freedom of expression and new media in Asia

In the aftermath of the Second World War, reconstruction and development took priority over political expression and participation. The rapid economic growth of many Asian economies in the 1980s and the rise of an urban middle class did not result in democratic change. Instead advocates of 'Asian Values' argued that democracy and human rights standards were culture-specific. The economic growth of the Asian economies was seen to validate the 'Asian way' of strong government, social conservatism and free market economies.

The Asian financial crisis of 1997 exposed the institutional weaknesses in the region, and generated the space for economic and political reform. In general terms civil society held the potential to require transparency and accountability from Asian governments. The spread of the internet, the English language, cheaper international telephone charges and global air travel were additionally put forward as contributors to democratic reform (Gomez and Smith, 2003).

The expansion of freedom of expression and the decline of censorship has often been associated with the movement towards democracy. While some agree that in Asia there has been some movement towards democracy (AMIC, 2000), it is unclear whether this involves a decline of censorship and an increase in freedom of expression. Historically much of the law and methods of government media control in the region originated from colonial regimes. Strict regulation of the media, especially with regards to political content, has been the consistent feature. The containment of freedom of expression has involved the use of legislation to restrict access, the proscription of content, the exercise of influence through ownership and the inducement of self-censorship. These measures were supplemented by surveillance from the police, military and selected arms of the state bureaucracy. Tactics ranged from low-tech letter opening and the use of informants to (what was then) high-tech telephone tapping.

The emergence of the internet in Asia during the early 1990s, raised the possibility that public discourse could take place without the mediation of licensing authorities, and the gate-keeping and agenda-setting of the mass media. Technically, individuals could communicate with each other across geographical and political boundaries without restriction, and the movement of text was hard to control. Consequently, traditional media censorship was seen to have an uncertain future on the internet. Many observers were confident that any attempt by authorities to protect data, monitor content or censor information could be circumvented by the use of re-routing and avoidance measures. In this regard, there were expectations that freedom of expression would increase and further democratic development in the region.

It is naïve, however, to equate new media technologies with democracy. The crucial ingredients for establishing a functioning democracy are an active citizenry, a vibrant civil society and a state that enables access to information, privacy, human and civil rights. Many observers forget that oppositional activism in one form or another always confronts arbitrary power. Authoritarian regimes in Asia, for example, monitor and restrict the opportunities for activists to use traditional methods of communication such as pamphleteering, newspaper publishing, community radio, print and broadcast media. With the advent of new information and communication technologies activists can now avail themselves of a variety of online and mobile communications tools. They use these tools to mobilise people for action around a cause or issue, making them cyber-activists. In response conservative regimes make new laws to monitor internet usage and place restrictions on activists who use new technologies for the purposes of advocacy.

Meanwhile several studies have concluded that initial euphoria concerning the democratic potential of the internet was misplaced. It is now evident that information technology alone cannot introduce democracy (Kalathil and Boas, 2003). Consequently the internet is not necessarily a threat to authoritarian regimes. Other writers note that social engineering, de-politicisation and self-censorship generate a politically apathetic and fearful citizenry that is reluctant to use the internet to its optimal potential (Banerjee, 2003).

At the same time the internet is continually re-inventing itself and its potential to contribute towards democratic change cannot be judged prematurely. The internet's inherent capacity for collaboration and information sharing, the onset of wireless technology and the growth of 'blogging' indicate the opportunities for democratic activism in Asia and elsewhere. In this regard, desktop computers have been making way for laptops and pocket PCs. This merging with mobile phones is putting more computing power into hand-held devices. Hence, new media developments remain a concern for conservative regimes

The beginnings of internet censorship in Asia

In Asia pornography, hate speech and, later, gambling were early targets of web-based censorship and remain ongoing themes of concern for legislators in the region.

In 1996 the Chinese authorities legislated against pornography on the

Internet (State Council Order No.195, 1 February 1996). Online pornography was also prohibited under Article 5 of the *Computer Information Network and Internet Security, Protection and Management Regulations* (December 1997), Article 57 of the *Telecommunications Regulations Of The People' s Republic Of China* (25 September 2000) and the *Measures For Managing The Internet Information Services* (25 September 2000). ASEAN representatives discussed a possible common framework and regional body to restrict pornography on the internet (Menon, 1999). Such measures are often complicated by varying definitions of 'pornography' and by moralistic censorship regulations. An internet content rating system introduced to Hong Kong in 2001, for example, classified gay and lesbian websites as 'harmful media'. The owner of the first and biggest gay website in the country was told to mark it as a 'harmful site' and install filtering software to prevent youth access. Failure to do so would risk imprisonment. The legislation has come under heavy criticism by rights groups including Amnesty International (Amnesty International, 2002). Similarly under the *Indian Information Technology Act 2000*, the Indian Government also declared electronic publication of pornography an offence (see Chapter XI Para 67).

More recently, Asian governments have moved to restrict online gambling. Some have looked to supplement existing legislation prohibiting gambling with specific measures to combat online gambling. On 18 February 2003 prosecutors and police raided the offices of a Taiwan advertising company that had helped promote business for British internet sports betting company Sportingbet. A Taipei prosecutor recently indicted Dai Chi-feng for helping to transfer local gamblers to casinoluxy.com through a super link. Both actions were based on existing regulations in the *Criminal Code* that penalise people who instigate others to commit crimes or make profits by engaging in gambling (*China Post*, 2003). In 2002, China announced restrictions on internet cafes under which customers were banned from looking at websites offering prostitution, adult entertainment or gambling (Gambling Licenses Online, 2002). During 2003 legislators in South Korea discussed law revisions subsequently introduced to the National Assembly which prevented PC rooms and internet cafes from providing gambling or other betting services (*The Korea Times*, 2003).

There have also been attempts to restrict websites that promote hatred of ethnic and religious groups. Section 4(2)g of the *Singapore Internet Code of Conduct* prohibits material that 'glorifies, incites or endorses ethnic, racial or religious hatred, strife or intolerance.' Article 5 of the *Chinese Computer Information Network and Internet Security, Protection and Management Regulations*, December 1997, purportedly protects 'nationalities'. In September 2002, a website in Australia was ordered by the Federal Court to remove material that casts doubt on whether the Holocaust occurred. Judge Catherine Branson ruled that Dr Toben vilified Jewish Australians when he published documents that cast doubt over the Holocaust on the Adelaide Institute website (*The Australian*, 2002).

Legislation is not the only measure taken against such sites. Active technological 'blocking' of sites is also another option employed by governments. For instance in Thailand, the Government filters access to internet content by using a caching proxy server which delivers a 'request denied page' instead of the one sought by the internet user. Thai ISPs receive official guidance from the Ministry of Information and Communications Technology via a periodic 'BlockURL' message. This lists domains that ISPs are supposed to look out for and block. About 1250 sites are blocked, most are pornographic, a few are devoted to online gaming, and one belongs to a separatist movement (Ignotus, 2004).

Another emerging issue is spam – unsolicited email messages. Asian countries are looking towards countering it, with front runner Singapore considering specific anti-spam legislation to guard against unsolicited email. Currently, spammers who continue after their ISPs receive complaints will be 'given the boot'. In cases such as a deliberate and malicious 'mail-bombing' campaign, the spanner can be charged under the *Computer Misuse Act* and fined up to $S10,000 with a three-year prison sentence (*Computer Times*, 2003). While it might appear that such legislation is directed against unsolicited commercial emails, there are also political implications. Many NGOs and political parties use mailing lists to reach out to people in restrictive environments. Spam legislation allows governments to criminalise people or organisations that send out email notices to individuals who claim that they had not specifically asked to be put on mailing lists. Spam messaging on mobile phones is also a growing trend in Asia as marketers use text messages to target subscribers. In Japan, this occurs where SMS spammers generate at random the email style addresses used for text messaging. NTT DoCoMo, Japan's largest mobile phone company, is taking legal action against spammers by cutting off more than 2000 lines because of spam abuse. It has also sought damages in some cases (Young and Kane, 2004).

Censoring online political content

While it is true that governments in Asia were interested in developing the economic dimension of the internet these same governments were also mindful of the political challenge that the internet might pose (Ho et al., 2003). Their legislation against political users of the internet reveals several trends.

Suppressing political expression

Authoritarian regimes in China and Vietnam have imposed numerous restrictions on cyberspace, using firewalls and arresting cyber-dissidents (Neumann, 2001). In this regard, Vietnam remains one of the world's most repressive countries; websites that are considered politically and morally dangerous (including foreign news sites and those of human rights organisations) are blocked by the Government. It is officially forbidden to use the internet for political opposition, for actions deemed contrary to national sovereignty, national security, morality or the law. Violators of this regulation are often punished with imprisonment for several years. The government has plans to make internet café owners responsible for their customer's messages and to set up a national monitoring system to ensure that cyber café users don't see 'politically or morally dangerous websites' (RSF, 18 June 2003).

Several cyber-dissidents have been arrested, harassed or placed under house arrest for publishing religious texts or critiques of the Government (Free Vietnam Alliance, 2002). In January 2004, there were nine cyber dissidents in prison or under house arrest (RSF, 2004). Nguyen Vu Binh, for example, a former journalist who used the internet to criticise the Government, was arrested in an internet café in Hanoi on 21 February 2002, after posting an article in which he criticised Vietnamese-Chinese border agreements signed in 1999. He was held in detention without trial until he was sentenced to prison on 1 January 2004 for seven years (Index On Censorship, 2004). On 20 December 2002, cyber-dissident Nguyen Khac Toan was sentenced to 12 years in prison after he was 'found guilty of spying for emailing material to allegedly "reactionary" Vietnamese human rights organisations abroad'. He was arrested in a Hanoi internet café on 8 January 2002 (IFEX, 2003).

The Chinese Communist authorities use a variety of tools to repress free expression on the internet. These include harsh laws, stiff jail sentences, crackdowns on internet cafés and the blocking of many 'subversive' websites, such as those of CNN, BBC and Human Rights Watch. As of December 2003, at least 48 Chinese citizens had been arrested for expressing their opinions through the internet (IFEX, 2003). For example, Kong Youping, a factory worker, was arrested on 13 December 2003 at his home for posting political articles and poems on foreign websites over the previous six months (China Study Group, 2003). Another Chinese activist, He Depu, was sentenced to eight years in prison on 6 November 2003 for collaborating with the Chinese Democratic Party and posting messages on the internet 'inciting subversion' (IFEX, 2003).

The military junta in Burma has effectively barred all internet social activity and is only now beginning to allow access to a limited package of approved websites, referred to as the 'intranet' (Lintner, 2001). Even then, to a get a private connection to the internet a licence is required and high fees are charged. The initial activation costs $US260 and a monthly fee of $US35 for 20 hours usage has to be paid (Zaw Oo, 2004). In addition these fees are in Foreign Exchange Certificates (FEC) rather than in local currency. Most people cannot afford these costs; thus internet use is beyond the reach of the general population. The number of cyber-cafés is also limited because prior approval via a licensing system is required. Within each cafe, customers are not allowed to access free email services such as Hotmail or Yahoo.

Legislating against electoral use of the internet

Singapore has sought to comprehensively restrict electoral internet space. It passed a bill in 2001 to amend the Parliamentary Elections, before the last elections in 2002. The Government set the boundaries on political campaigning over the internet by barring the publication of survey and poll data. Political web sites can publish party posters and manifestos, candidate profiles, party events and positions on issues, and some moderated chats and discussion forums. On the barring of election surveys and exit polls, the minister said these gave the illusion of reflecting public opinion but were often based on small sample sizes, bad question design and improper sampling, which led to inaccurate and slanted results. Opposition leaders said the new law was designed to curb their efforts to reach the electorate via the internet (Wong, 2001).

In Japan, the Government has taken steps to deal with the internet as a medium for political campaign activities by applying 'existing media-use legislation in the form of the Public Offices Election Law (POEL) to political content that is aimed at the electorate during official election campaign periods'. Due to the POEL and its wide range of regulations, Japan's electoral system has been described as one of the strictest in the world. Its strictures constrained opposition parties from actively campaigning on the internet during the 1998 Upper House election, but non-traditional political actors and individuals emerged during the campaign, signaling an important trend. These political actors established email newsletters, bulletin-board services, chat groups, ideologically neutral portal sites, as well as 'anti-candidate' websites. All of these circumvented the POEL. Unlike legislation in Singapore, the POEL did not cover email communications, giving political parties and some candidates the leeway to send email bulletins to subscribed members throughout the official campaign period for the 2001 Upper House election (Tkach-Kawasaki, 2003).

In Korea the high number of broadband subscribers enable civic groups, political parties and politicians to routinely use the internet. The home pages of political parties, politicians, citizen groups become especially active during election campaigns. However the law says little about the internet and politics during such periods and this caused some problems in the 2002 presidential campaign. For instance, the online media Ohmynews' attempts to hold 'relay interviews' with the front runners of the 2002 presidential election candidates was seen to violate Article 254 of the *Elections Act* because the law prohibits non-press media from having live forums just before the official campaign period (Kyu, 2003). However, this was seen as being out of sync with developments in new technology. Hence, unlike Singapore or Japan, plans were made for positive legislation in 2003 to enable more online politicking during electoral campaign periods. Nevertheless, discrimination against online news portals remains. For instance it is well-known that Government offices' press clubs are not open to internet reporters (Kyu, 2003).

Terrorism related suppression and legislative measures

Attempts to regulate the internet include legislation as well as policing and suppression activities designed to restrict internet usage (e.g. surveillance, filtering, website closures and the shutting down of cyber-cafés).

Under the label of 'fighting terrorism', the Pakistani Government has taken measures that reduce the privacy of internet users. Since August 2002 cyber café owners in Pakistan have been compelled to record the names, connection times, numbers called and computer identities of their customers. According to officials these records will help track down terrorists by making emails easier to trace and this will promote security. The Government announced that monitoring internet use would be necessary for Pakistan's anti-terrorism efforts. Several websites have been blocked; an al-Qaeda website and other pages that provide 'anti-Islamic' or 'blasphemous' information (RSF, 18 June 2003; Index On Censorship, 6 August 2002).

In Bombay, Indian police are proposing a regulation requiring customers to show photo identification and give their addresses whenever they patronise any of the city's 3000 cyber-cafés. Cyber-café owners would have to retain these records for up to a year and show them to police on request. Authorities are fearful that terrorists and other criminals are taking advantage of cyber cafés to communicate via email and the internet. The police have enlisted the help of technology experts and internet service providers to trace emails in order to track down terrorists. Although very few countries regulate internet cafes it certainly is an emerging trend. But reports from the ground suggest that rigour behind the record keeping varies. In some instances, anyone can walk into a cyber café, scribble an illegible name and still get access to the internet.

To prevent people obtaining communication services anonymously, Australian authorities no longer allow pre-paid cards for mobile phones to be sold without identification over the counter. Convenience stores, petrol kiosks and university campus shops which sell a variety of pre-paid mobile telephone cards (for companies such as Optus and Telstra) require buyers to produce a photo ID; usually a driver's licence. They must also indicate a local address and phone number on a purchase form before the vendors can sell a pre-paid card. However, account top-up cards can be purchased freely without a need to present any ID. In countries such as Thailand, both pre-paid mobile telephone cards and the corresponding top-up cards can be purchased without the need to present any ID to vendors.

The Philippines and Indonesia, are preparing legislation to exercise control over users of communication devices and services. The Philippines' draft *Anti-terrorism Bill* proposes measures to sanction arrests without court orders, initiate 30-day detentions without change, among others. It would also allow the Secretary of Justice to authorise wiretaps, including those of internet communications (Privacy International and the GreenNet Educational Trust, 2003). In order for wiretaps to work, there needs to be a certain amount of cooperation between law-enforcement agencies, telecommunications companies and internet service providers. Such co-operation is also required in cases where the authorities want to monitor certain user accounts. No one is sure of the extent of this cooperation (Pabico, 2003). In late 2002 a Mobile Patrol Group (MPG) policeman traced a 17-year-old who had called up a police station with a bomb threat. In this instance it was a simple case of the police hotline 116 being equipped with caller ID (SunStar Network Online, 20 October 2002). The police simply went to the teenager's house and apprehended him.

After the Bali bombings in 2002, Indonesia passed an *Anti-Terrorism Law*. The 'security forces can now intercept and examine information that is expressed, sent, received or stored electronically or with an optical device, and can detain anyone for up to three days without evidence'. They can thus intercept emails and tap telephones (Luwarso, 2003). Apart from law, the perceived threat of terrorism has led to the use of high-tech tracking devices in the search for terrorist suspects. In late 2002, Indonesian police using technology which requires only seconds to identify the location of a cellphone, arrested Imam Samudra who later confessed that he was the chief planner and coordinator of the Bali bombings (Elegant, 2002). It was reported again in mid-2003 that the Indonesian police used similar mobile-phone tracking technology to track and arrest members of the Jemmah Islamiah following the Bali bombings (Elegant, 2003). This suggests that internet communication between handheld devices can be effectively put under surveillance and traced.

Cyber security conferences

Initially most cyber security conferences in Asia dealt with issues like e-commerce, virus protection, prevention of hacker attacks and a safe online business environment for companies and their customers. Such conferences also cover cyber stalking, internet hour theft, data theft, cyber blackmail, defamation of individuals and nations, and corporate espionage. Concern over 'cyber terrorism' was secondary. Since September 11 however, capacity-building to counter cyber criminals has been stepped up through a series of regional cyber security conferences. These are often supported by the United States but jointly organised with the various local partners.

One example stems from the early cooperation between the US Federal

Bureau of Investigation (FBI) and the Indian Central Bureau of Investigation (CBI) in 2000 to fight cyber crime in India. After FBI experts had trained Indian policemen to handle computer crimes, the Indian CBI went on to establish its own cyber crime unit. (BBC News, 23 July 2000) In February 2004, the CBI announced that it would soon begin networking with nine other Asian countries through a 'Cyber Crime Technology Information Network System' (CTINS). This was initiated by the National Police Agency of Japan (newindpress.com, 2004). In 2003, Pakistani 'Federal Investigation Agency' (FIA) officers were trained to fight cyber crime by the US Federal Bureau of Investigation. The new FIA unit, named 'National Response Center for Cyber Crimes' (NR3C), was set up to deal with cyber crimes in Pakistan and included plans to create a cyber security net in the country (Computer Crime Research Center, 2003).

A conference on strengthening international law enforcement cooperation to deal with cyber crime, was held in July 2003 by the Asia Pacific Economic Cooperation (APEC) eSecurity Task Group. The primary conference objectives were as follows: to assist countries to develop the legal frameworks necessary to combat computer crime; to provide law enforcement investigative units with training and equipment to investigate and deter computer crime; and to enhance cooperation between industry and law enforcement in order to confront computer crime (APEC, 25 July 2003). A related APEC initiative is the 'Cybersecurity tool kit' which is to be developed jointly with several business organisations including Microsoft. This 'kit' will enable businesses to implement appropriate security measures to protect their systems. Businesses are also being encouraged to work with law enforcement agencies to investigate cyber crime (APEC, 8 October 2003). Although aimed at cyber criminals, hackers and virus authors, such measures can be used to prosecute pranksters and legitimate cyber-activists.

Unsurprisingly, therefore on 19 September 2003, the Association of South- East Asian Nations agreed to intensify its efforts to fight cyber crime, hackers and computer viruses. ASEAN has set up a framework to share information in order to respond to incidents like fast spreading viruses or other forms of 'cyber crime'. Each member country has set up a 'Computer Emergency Response Team' (CERT) to coordinate the cooperation. ASEAN plans to intensify and expand the information sharing in the coming years (Reuters). These measures can be traced back to May 2002 when ASEAN Member countries agreed on a work programme to implement the 'ASEAN

Plan of Action to Combat Transnational Crime'. This work programme includes the online exchange of information on cyber crime activities via the ASEAN Secretariat as well as the sharing and analysis of critical intelligence information. Member countries also agreed to develop regional training programmes and conferences to enhance existing capabilities for the investigation, intelligence, surveillance, detection and monitoring of cyber crime on the internet. Members agreed to exchange their 'best practices' in fighting cyber criminals, including ways of tracking down emails.

In February 2004, plans were announced for a new Centre for Law-enforcement Cooperation in Jakarta (Go, 5 February 2004). The centre will facilitate information sharing on terrorist activities as well as conduct training sessions for police from Asia-Pacific countries in counter-terrorism skills (Go, 6 February 2004). The centre, a joint Indonesian-Australian effort, was discussed during a two-day conference in Bali in early February. Twenty-five countries from the region attended and there was high-level US participation.

The problem with such capacity building is that shared expertise may be abused by certain governments if there are no checks and balances to protect the privacy of individuals. Such a possibility conforms with the pattern of control over the traditional media exercised by many Asian regimes.

Surveillance and storage of data traffic

Central to the control over internet content is state ownership or regulation of ISPs (technologies that enable internet users to be traced to their computers) and the increased inter-state pooling of surveillance information. In Asian countries cyberspace is a realm for surveillance. According to Lyon (2003), surveillance is 'focused attention on behaviours and trends of persons and of populations with a view to managing, controlling, protecting, or influencing them'. Like elsewhere, the internet is used in Asia for repressive and illiberal purposes, and surveillance is the norm with its emergence as a 'medium for commercial, management, policing, and government activities' (Lyon, 2003).

Online surveillance is carried out by both governments and corporations. The governments of South Korea, Japan, Singapore and Hong Kong, for example, require internet service providers to keep information on users and to help law enforcement agencies track their online activities. In Japan, the Communications Interception Law was passed in August 1999, allowing law enforcement officials access to private e-mail accounts if they were investigating certain types of crime (Williams, 2000). By law the Communications

Authority of Thailand (CAT) has a minimum 32 per cent share in all privately-owned ISPs. In addition the National Information Technology Committee (NITC) has ordered ISPs to retain connection data about their customers for at least three months. This will enable prosecutors to act against those who log on to undesirable websites and it will encourage government authorities to block such sites. (Reporters Without Borders, 2002)

Similarly, handheld devices such as mobile phones are also subject to surveillance. In Singapore, the perpetrator of an unintentional bomb hoax via a mobile phone's short messaging system (SMS) was traced within two weeks of the incident. This was undertaken by the police with the cooperation of all three telecommunications companies – Starhub, M1 and SingTel. All of them store SMS messages in their servers or databases, for periods of time ranging from two days to a few weeks, before they are deleted (*The New Paper*, 2002, 2004). The police have powers to compel telecommunications companies to hand over information in their databases (*The New Paper*, 2002). Under the Telecommunications Act, those guilty of transmitting bomb hoaxes can be fined up to $50,000, jailed up to seven years, or both (Soh and Dawson, 2002).

Noting trends in the United States and the European Union, the International Chamber of Commerce (ICC) has strongly criticised government attempts to compel communication service providers to store end-user traffic data. According to the ICC this practice is neither economically efficient nor effective for criminal investigation. It has expressed concerns about end-users privacy and recommended transparent and effective oversight procedures to prevent abuses and to protect user confidence. More importantly, the ICC recognises that there has been insufficient public input and multi-lateral harmonisation. In its view this could impair a competitive and dynamic communications and IT services market (International Chamber of Commerce, 2003).

Authoritarian governments however cite 'national security' or 'internal order', and corporations justify their actions in terms of 'lubricating market mechanisms'. Accordingly, internet surveillance is promoted as 'necessary' in order to 'maintain strong states and to develop mature markets'. Accountability and the protection of privacy, however, is inadequate (Lyon, 2003).

Conclusion: Dumbing down democracy

Between 1998 and 2000 online political activity emerged and grew. In response it has taken some countries a while to introduce specific cyber-legislation and impose restrictions. It was not until 2000 that the Indian government passed the *Information Technology Act*. Authorities in Cambodia have so far made no efforts to regulate or restrict the internet, and Malaysia stands by its promise not to censor internet content. The lack of restrictions in these countries results from indifference because of a low level of internet penetration (thus making the medium irrelevant as a tool of political dissent). In the case of Malaysia, the Government's position stems from a desire not to deter foreign investment.

By the year 2000 there were signs that restrictions upon political cyber activism were about to emerge; this became the dominant trend subsequent to 9-11. Political expressions that blossomed with the arrival of the internet are being brought under legislative control. As a result, the internet itself has become a target for censorship, regulation and control.

However, the absence of specific regulations governing the internet has not prevented governments from using other legislation and intimidation to control internet content and cyber-dissidents. In many Asian countries the new possibilities for free expression that accompanied the advent of the internet still carry the old risks of persecution (Menon, 2001). The repressive practices of media control, from the colonial era to post-colonial and contemporary governments, have been applied to the internet and the information carried by mobile information devices. Thus, to a large extent, the cyber security measures resulting from the 'war against terrorism' are simply an extension of existing censorship laws and surveillance strategies.

Hence, we can question the argument that the media occupies a key position in the development of democracy. If we regard the internet as an extension of the mass media (in that it offers one-to-many communication via websites and email lists) then democratic hopes appear misplaced. Given the increased legislation against it, new media is not as free as it was originally deemed to be.

Democracy requires a public culture of participation, but the stringency of post September 11 internet-related legislations seems to generate the opposite tendency. People are more reluctant to conduct political communication online if it can be monitored by state agencies with the cooperation of commercial service providers. Hence, people prefer to keep important information confidential and communicate in a low-tech or no tech manner. This is especially so under authoritarian regimes such as Burma, Vietnam and Singapore. In fact, many surveys show that the percentage of websites and news groups oriented towards politics is rather small. It has been observed that key institutions central to democracy such as political parties have become irrelevant in late modernity. In this view, official politics does not command the level of support and/or participation that it did in the past. Indeed politics itself is fragmenting, and the activist focus moves outside the formal political process toward social movements, civil society and NGOs. But if the internet does not live up to the demands of 'new politics', then old-style low tech political organising will still be relevant.

Consequently traditional activism will still be required to get around the high-tech surveillance state. At the same time, new media technologies can be useful if human beings use them with ingenuity and determination. This underlines the central importance of the 'people' and their willingness to act.

It remains to be seen if further innovations in information technology will allow cyber activists to bypass tighter government control. In the meantime the repressive tendencies I have outlined serve to confirm that the democratic potential of the internet is being dumbed down.

References

Amnesty International. (2002). Internet Restrictions: stifling freedom of expression from China to Tunisia, www.web.amnesty.org/mavp/av.nsf/pages/internet#south_korea

APEC media release. (2003). Conference on the Strengthening International Law Enforcement Cooperation to Prosecute Cyber Criminals, Hackers, and Virus Authors, Bangkok, July 25. www.apecsec.org.sg/apec/news___media/media_releases/250703_tha_strengthening_law.html

APEC media release (2003). APEC Cybersecurity Tool Kit to be Developed for Corporations and SMEs, Chinese Taipei, October 8.

www.apecsec.org.sg/apec/news___media/media_releases/081003_ct_cybersecurity.html

ASEAN. (2002). Work Programme to Implement the ASEAN Plan of Action to Combat Transnational Crime, Kuala Lumpur, May 17.

202.154.12.3/5616.htm

Asia Media Information & Communication Centre. (2000). Media and Democracy in Asia, Singapore: AMIC.

The Australian (2002, September 18). Court bans racist website.

australianit.news.com.au/common/print/0,7208,5119879%5E16123%5E%5Enbv%5E,00.html

Ayers, M. C and M. McCaughey. (2003). Introduction. In Martha McCaughey (ed.), *Cyberactivism: Online Activism in Theory and Practice*, New York & London: Routledge.

Badam, R. T. (2004, January 18). Police in India to monitor cybercafes, Boston.com www.boston.com/business/technology/articles/2004/01/18/police_in_india_to_monitor_cybercafes/

Banerjee, I. (2003). Internet and democracy in Asia: a critical exploratory journey In Indrajit Banerjee (ed.), *Rhetoric and Reality: The Internet Challenge for Democracy in Asia,* Singapore: Times Media Private Limited.

BBC News. (2000, July 23). India tackles cyber crime. news.bbc.co.uk/1/hi/world/south_asia/847727.stm

Boas, T. C and Kalathel, S. (2003). *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule*, Washington DC: Carnegie Endowment for International Peace.

China Post (2003, February 19). Offices of Sportingbet's Taiwan promoter raided. www.chinapost.com.tw/taiwan/detail.asp?ID=35102&GRP=B

China Study Group. (2003). China arrests factory worker who posted political essays online, December 20. www.chinastudygroup.org/index.php?type=news&id=4064

Chua, H. (2003). Anti-spam laws in the making?, *Computer Times Online*, October 29. computertimes.asia1.com.sg/news/story/0,5104,1497,00.html

Committee to Protect Journalists. (2002). China: college student missing after posting essays online. www.cpj.org/news/2002/China10dec02na.html

Computer Crime Research Center. (2003, July 11). FBI training FIA officers on cyber crime. www.crime-research.org/eng/news/2003/07/Mess1101.html

Dahlgren, P. (2001). The transformation of democracy? In Barnie Axford and Richard Huggins (eds.), *New Media and Politics*, London: Sage.

Elegant, S. (2003, May 5). Calm in the storm, *TimeAsia*.

Elegant, S. (2002, December 2). Where will they strike next?, *Time*.

Free Vietnam Alliance. (2002). Vietnam: new threats to free expression, October 9. www.fva.org/200210/story03.htm

Gambling Licenses Online. (2002, November 15). China. www.gamblinglicenses.com/

Go, R. (2004, February 5). Asia-Pac gets new centre to fight terror, *The Straits Times*.

Go, R. (2004, February 6). 25 nations unite on cross-border terror, *The Straits Times*.

Gomez, J. and A. Smith. (2003). Introduction. In Uwe Johannen, Alan Smith and James Gomez (eds.), *September 11 and Political Freedom: Asian Perspectives*, Singapore: Select Publishing.

Ho, K.C., R. Kluver, and K. C. (2003). Asia encounters the Internet. In K.C. Ho, Randolph Kluver and Kenneth C.C. Yang (eds.), *Asia.com: Asia Encounters the Internet*, London and New York: RoutledgeCurzon.

IFEX. (2003, January 3). Cyber-dissident Nguyen Khac Toan sentenced to 12 years in prison. www.ifex.org/fr/layout/set/print/content/view/full/18217/

IFEX. (2003, December 23). Cyber-dissident Kong Youping arrested; court rejects appeal hearing for dissident He Depu. www.ifex.org/en/layout/set/print/content/view/full/55812/

Ignotus, M. (2004, February 15). Censoring the Web, *Bangkok Post*, 15 February.

Index On Censorship. (2002, August 6). Pakistan: keeping tabs on web users. www.indexonline.org/indexindex/20020806_pakistan.shtml

Index On Censorship (2004, January 6). Vietnam: online dissident journalist jailed. www.indexonline.org/indexindex/20040601_vietnam.shtml

India Information Technology Act. (2000). www.mit.gov.in/itbillonline/it_framef.asp

International Chamber of Commerce (2003, June 4). Common Industry Statement on Storage of Traffic Data for Law Enforcement Purposes.

The Korea Times. (2003, March 10). Law revision bans gambling at PC rooms, Internet cafes. times.hankooki.com/lpage/nation/200303/kt2003031017174011980.htm

Kyu H. Y. (2003). The Internet and Democracy in Asia. In Indrajit Banerjee (ed.), *Rhetoric and Reality: The Internet and Challenge for Democracy in Asia,* Singapore: Eastern Universities Press.

Lintner, B. (2001). Denial of access. In Sheila Coronel (ed.), *The Right to Know: Access to Information in Southeast Asia*, Philippines Center for Investigative Journalism, pp. 21-41.

Luwarso, L. (2004). Manufacturing control: new legislations threatens democratic gains in Indonesia.In Steven Gan, James Gomez and Uwe Johannen (eds.), *Asian Cyberactivism: Freedom of Expression and Media Censorship*, Bangkok: Friedrich Naumann Foundation.

Lyon, D. (2003). Cyberspace, surveillance, and social control. In Ho, K.C., Kluver, Randolph, Yang, Kenneth C.C. (eds.), *Asia.com: Asia encounters the Internet*, London: RoutledgeCurzon.

Menon, K. (2001). Asia 2001 Overview, Committee to Protect Journalists (CPJ). www.cpj.org/attacks01/asia01/asia.html

Menon, V. (1999). Informatik Forum 1/99: Internet in Asia. www.interasia.org/results/if9901preface.html

Neumann, A. L. (2001). The great firewall, Committee to Protect Journalists. www.cpj.org/Briefings/2001/China_jan01/China_jan01.html

Newindpress.com. (2004, February 4). CBI tie up with Asian countries to fight cyber crime.
www.newindpress.com/Print.asp?ID=IEH20030206124234,

The New Paper. (2002, December 19). Your SMS is private, telcos say.

The New Paper. (2004, February 2). Service provider: SMS confidential but….

Pabico, Alecks P. (2003). New media as big brother: the Philippines after September 11. In Steven Gan, James Gomez and Uwe Johannen (eds.), *Asian Cyberactivism: Freedom of Expression and Media Censorship*, Bangkok: Friedrich Naumann Foundation.

PRC Interim Regulations Governing the Management of International Computer Networks. (1996). People's Republic of China, State Council Order No. 195, Article 13.

Privacy International and the Electronic Privacy Information Center. (2002). *Privacy and Human Rights 2002: An International Survey of Privacy Laws and Developments*. www.privacyinternational.org/survey/phr2002/

Privacy International. (2003). Privacy and Human Rights 2003: Executive Summary. www.privacyinternational.org/survey/phr2003/executivesummary.htm

Reporters Sans Frontieres. (2002). Vietnam annual report 2002. www.rsf.org/article.php3?id_article=1429

Reporters Sans Frontieres. (2002, September 5). 11 September 2001 – 11 September 2002: The Internet on Probation: Anti-terrorism drive threatens Internet freedoms worldwide. www.rsf.fr/article.php3?id_article=3671

Reporters Sans Frontieres. (2002. March 26). Torture, Arbitrary Detention and Self-Censorship. Four Months Later: Consequences of the State of Emergency and of the Fight Against 'Maoist Terrorism' Attacks on Freedom of the Press. www.rsf.fr/article.php3?id_article=902

Reporters Sans Frontieres. (2003, June 18). Pakistan press release. www.rsf.org/print.php3?id_article=7245

Reporters Sans Frontieres. (2004). Press Freedom Barometer. www.rsf.fr/rubrique.php3?id_rubrique=119

Reporters Sans Frontieres. (2004, January 6). 2003, a black year. www.rsf.org/article.php3?id_article=8969

Reporters Sans Frontieres. (2003, June 18). Thailand press release. www.rsf.org/print.php3?id_article=7251

Reporters Sans Frontieres. (2004, June 18). Vietnam press release. www.rsf.org/print.php3?id_article=7252

Rozumilowicz, B. (2000). Democratic change: a theoretical perspective. In Gunther, Richard and Mughan, Anthony (eds.), *Democracy and the Media: a comparative perspective,* London and New York: Routledge.

Singapore Internet Code of Conduct. (1997). www.sba.gov.sg/sba/i_codenpractice.jsp

Soh, N and Dawson, S (2002, November 30). Fear for safety fuelled SMS bomb hoax, *The Straits Times.*

SunStar Network Online. (2002, October 20). PNP goes on alert, traces 'prankster'.

Tharoor, S. (2003, October 17). The 'cyber summit': a chance to expand the information society, *International Herald Tribune.*

Tkach-Kawasaki, L. M. (2003). Clicking for votes: assessing Japanese political campaigns on the web. In K.C. Ho, Randolph Kluver and Kenneth C.C. Yang (eds.), *Asia.com: Asia Encounters the Internet*, London and New York: RoutledgeCurzon.

USA TODAY. (2003, September 19). South East Asia unveils cyber crime fighting plan.
www.usatoday.com/tech/world/2003-09-19-asean-on-cybercrime_x.htm

Ward, M. (2004, January 21). Snooping industry set to grow, BBC News World Edition. news.bbc.co.uk/2/hi/technology/3414531.stm

Williams, M. (2000, August 16). Japan's police gain right to tap phones and e-mail, CNN.com.
www.cnn.com/2000/TECH/computing/08/16/japan.police.idg/

Wong, J. (2001, August 13). Singapore limits election politics on internet, Reuters. www.singapore-window.org/sw01/010813re.htm

WSIS Declaration of Principles. (2003). Building the Information Society: a global challenge in the new Millennium, Geneva, December 12. www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!MSW-E.doc

Young, D. and Kane, Y. I. (2004, February 3). How spammers are targeting mobile phones in Asia, Reuters.
sg.news.yahoo.com/040203/3/3hpt1.html

Zaw O. (2004). Mobilising Online: the Burmese cyber strategy against the Junta. In Steven Gan, James Gomez and Uwe Johannen (eds.), *Asian Cyberactivism: Freedom of Expression and Media Censorship*, Bangkok: Friedrich Naumann Foundation.

James Gomez is a writer and an activist. He founded the Think Centre (Singapore) www.thinkcentre.org *in 1999 and his book,* Internet Politics: Surveillance and Intimidation in Singapore *was published in 2002. Gomez is also co-editor of* Asian Cyberactivism: Freedom of Expression and Media Censorship *(2004). Between 1998 and 2004 he was regional research and communications manager of the Friedrich Naumann Foundation's regional office, Thailand. He joined Monash Asia Institute as a doctoral candidate in 2004. This article was revised from a paper presented at the Centre for South-East Asian Studies Seminar series, Monash Asia Institute, Monash University on 11 March 2004.*
jamesgomez@hotmail.com
www.jamesgomeznews.com