Asia Overview

Asian cyberspace is the setting for a diverse range of information controls, contestations, and resistance. Governments across the region struggle to balance the rapid growth of information communication technologies (ICTs) with their concerns over social stability, national security, and cultural values. These tensions manifest themselves differently according to each state's context. The region is home to some of the least connected countries, such as Burma, and burgeoning ICT markets such as China and India. The spectrum of information controls across the region varies as well, with some of the world's strictest regimes of information control on one end and relatively unfettered communication environments on the other.

The continued growth of Internet connectivity in Asia, particularly in the mobile realm, has occurred alongside a growth in states' ability to monitor and control the flow of information. Countries such as Bangladesh, Indonesia, and Malaysia have seen dramatic increases in connectivity rates and mobile telephone ownership. However, as connectivity grows, so does the legal, regulatory, and technical capacity for states to monitor it. Both democratic and authoritarian states alike have expanded the scope of content that is considered illegal and have increased mechanisms to control it.

These have taken the form of centralized filtering mechanisms, increased power for regulators to monitor and censor content, and the prosecution of violators of content dissemination laws.

In 2009–2010, the OpenNet Initiative (ONI) conducted in-country testing of Internet filtering in Bangladesh, Burma, China, India, Indonesia, Malaysia, Pakistan, the Philippines, Singapore, South Korea, Thailand, and Vietnam. Testing results remain largely consistent with 2007–2008 findings and show that a spectrum of information filtering continues across Asian countries. Burma, China, and Vietnam maintain the most pervasive regimes of Internet filtering in the region, primarily targeting independent media and content related to politically sensitive issues, human rights, and political reform. On the other end of the spectrum, Singapore continues to symbolically block a limited number of pornography Web sites.

Filtering in South Korea and India focuses primarily on content related to national security and conflict issues—with South Korean Internet service providers (ISPs) extensively targeting online content related to North Korea and India targeting topics of Hindu extremism. Pakistan also focuses on blocking issues deemed sensitive to national security such as the Balochi conflict and independence movement, as well as religious content deemed blasphemous. Although previous ONI testing found no evidence of Internet filtering in Indonesia, recent testing revealed that ISPs are substantially filtering online pornography and selectively targeting political, blasphemous, and Internet-tool-related content. In Thailand filtering primarily concentrates on political content in reaction to sensitive events such as the 2009 political unrest that gripped the country. OpenNet Initiative testing found no evidence of Internet filtering in Bangladesh, Malaysia, or the Philippines.

Internet in Asia

Asia is home to one of the most connected countries in the world, and some of the least connected. In recent years, the region has seen tremendous growth, with several states identifying ICT growth as an integral part of their socioeconomic development. The mobile sector in particular has grown exponentially—an important development in countries with relatively underdeveloped fixed telecommunications infrastructure. In some countries, fixed infrastructure development has stagnated, eclipsed by the rapid rollout of mobile connectivity.

South Korea remains a world leader in Internet connectivity with one of the highest penetration rates and data transfer speeds in the world.[1] South Korea has penetration rates exceeding 81 percent[2] and an average broadband connection speed of 17 Mbps, the highest in the world and more than double the rate of second-ranked Hong Kong.[3] While not as high as South Korea, Malaysia also has a relatively substantial Internet penetration rate of 55.9 percent[4] and, like many in the region, a rapidly growing

mobile sector. Malaysia's mobile penetration rate in 2009 was 106 percent, with 21 percent of subscribers using 3G technologies.[5] Vietnam has seen strong growth in both fixed and mobile connectivity, with broadband subscription rates growing at more than 40 percent annually[6] for the past two years and mobile penetration rates estimated to exceed 140 percent by the end of 2010.[7]

China remains one of the most significant examples of the growth of the Internet in Asia. Although its penetration rate is relatively modest at 28.9 percent, its total of almost 390 million Internet users in 2009 makes it the largest Internet population in the world.[8] Much like its neighbors in the region, China has experienced a dramatic growth in the mobile telephone sector. From having less than 100 million mobile phones in 2000, the country is estimated to approach one billion phones by the end of 2011.[9] The gap between urban and rural connectivity rates mirrors that of some of its neighbors. A 2008 initiative by the Ministry of Information and Industry sought to narrow this gap, extending broadband services to 92 percent of rural townships.[10] Despite improving the number of rural users to over 100 million by 2009, low incomes and lack of access make Internet connectivity still a luxury for many.[11]

In contrast, Burma remains one of the least connected countries on record, with government restrictions, slow connection speeds, and prohibitive costs contributing to a penetration rate of only 0.2 percent.[12] Fixed broadband subscriptions numbered roughly 15,000, representing a penetration rate of 0.03 percent.[13] In Bangladesh, similarly, the government has launched initiatives to expand the ICT sector as a means of driving socioeconomic development, but access remains relatively limited.[14] Penetration rates are below 0.4 percent of the population, and the fixed broadband subscription rate is 0.03 percent.[15] Despite this low level of fixed Internet access, the mobile market is growing rapidly, with a 37 percent penetration rate.[16]

Although India's penetration rate is low at just over 5 percent,[17] the country is experiencing a surge in mobile access. From roughly 10 million subscribers in 2002, the mobile market is expected to exceed 750 million by 2011.[18] Pakistan has seen a similar boom in its mobile and wireless market. While overall Internet penetration rate is only 11.3 percent,[19] mobile penetration exceeds 60 percent.[20] Pakistan was also home to the world's first countrywide deployment of the next-generation wireless technology, WiMAX.[21]

The case of Indonesia demonstrates the contribution that mobile technology can make in an environment with expensive and limited fixed connectivity. Given that the monthly cost for fixed broadband can be more than five times that of mobile access, subscription rates for fixed broadband are below 1 percent.[22] Growth of mobile subscriptions, however, was expected to exceed 20 percent in 2010, leading to more than three-quarters of the population having a mobile phone.[23] Thailand has similarly seen the number of mobile subscriptions more than double between 2004 and 2009.[24]

Legal and Regulatory Framework

The regulatory and legislative capacity of states to filter content and prosecute individuals for online content has steadily grown. Many states in the region have increased monitoring of content, expanded the range of content deemed unacceptable, and prosecuted more individuals for violating content rules. This trend has not been limited to authoritarian states in the region; democracies such as India and South Korea have also expanded their capacities to regulate content.

Efforts undertaken by Asian states to expand the legislative, regulatory, and technical capacities for Internet filtering include the creation of new groups tasked with monitoring content, new powers for existing groups to block content deemed illegal, and expansion of governments' capacity to control filtering mechanisms. In October 2009 the Indian Parliament passed an amendment to the Information Technology Act, expanding the powers of the central government to block Web sites considered a threat to national security or public order.[25] This amendment also expanded the mandate of the Indian Computer Emergency Response Team (CERT-IN) to coordinate all cyber security issues and to enhance cyber protection.[26] The Pakistan Telecommunication Authority has proposed that they be given access to a centralized filter to more effectively block Web sites containing offensive content rather than relying on orders to individual ISPs.[27] Similarly, the Indonesian Ministry of Communication and Information Technology began drafting a bill that includes plans for a monitoring team tasked with ordering ISPs to block content deemed illegal.[28] Thailand has seen already-existing legislation applied more frequently. Since the 2007 passage of the Computer-Related Offenses Act, the number of orders to shut down Web sites has steadily increased. While only two URLs were ordered blocked in the year the bill was passed, nearly 44,000 were ordered blocked in 2009.[29] In 2010 the Chinese government amended the 1988 State Secrets law to include all ICT companies operating in the country, requiring them to cooperate with the state in cases where state secrets are allegedly leaked online.[30] The regulations would require companies to block the distribution of such information and disclose records to state security organs.[31]

Many governments have expanded rules that prohibit content deemed libelous, hateful, blasphemous, or causing insult to religious or other social groups. This type of legislation was instituted in Bangladesh during the period of emergency rule and has remained in place since. The Emergency Power Rules established in 2007 forbid the use of the Internet to publish "provocative" material, primarily aimed at content critical of the ruling government or army.[32] However, since the end of emergency rule, the Information Communication and Technologies Act still prohibits content that is "false and vulgar" or that "may harm religious feelings," among other restrictions.[33] A bill drafted in late 2010 sought to extend punishment for crimes related to distribution of pornography online.[34] Indonesia has similar prohibitions against defamation

in its Electronic Information and Transaction Law, which was unsuccessfully challenged in the Constitutional Court by a group of bloggers and media rights advocates.[35] Other sections of the same law prohibit dissemination of information intended to invoke hatred or hostility toward groups based on race, ethnicity, or religion, which caused the law to be invoked during the controversial "Everybody Draw Mohammed Day."[36] Controversy over the release of Indonesian celebrity sex videos led to a crackdown on pornographic Web sites and the government introducing the Trust Positive keyword-filtering system.[37] Pakistan has strict antiblasphemy laws, and the Supreme Court has ordered the Pakistan Telecommunication Authority to block access to Web sites with blasphemous content.[38]

This type of legislation is not unique to the authoritarian regimes of the region. South Korea's Telecommunications Business Act forbids communications that "harm the public peace and order or social morals and good customs."[39] Malaysia's Communications and Multimedia Act prohibits content deemed "indecent, obscene, false, menacing or offensive in character," with violators risking fines and jail time.[40] Filtering and takedown notices in Thailand also focus heavily on content deemed offensive, with the country's lèse-majesté laws targeting any negative remarks aimed at the monarchy. Combating this type of speech online has been deemed the top priority of Thailand's Ministry of Information and Technology.[41] More than three-quarters of the 75,000 orders blocking Web sites since the introduction of Thailand's Computer-Related Offenses Act in 2007 have been based on lèse-majesté laws.[42]

Alongside this increase in legislative and regulatory capacity has come the arrest of bloggers for content deemed politically sensitive, libelous, or against the public order. In Malaysia, numerous individuals have been charged for content posted online, including alleged insults to the monarchy[43] and the posting of a satirical article about the state power company.[44] In Bangladesh there have been several raids on television stations and newspapers critical of state officials, and journalists have been arrested for defaming the ruling government.[45]

Similarly, in South Korea individuals have been charged or investigated for posting online content identified as rumors, defamation, or misinformation. Online discussion following the sinking of a South Korean warship and the shelling of a South Korean island led to the arrest of several individuals charged with spreading "groundless rumors."[46] However, a December 2010 Constitutional Court ruling in the country may affect how such prosecutions are handled in the future. Following the acquittal of the blogger known as Minerva, the court ruled that the law under which bloggers had been prosecuted violated freedom of speech as guaranteed in the constitution.[47]

Numerous bloggers in China have also been imprisoned for posting content deemed controversial or politically sensitive. For example, a Twitter user was arrested for retweeting a sarcastic message about the recent naval conflict with Japan,[48] while an activist for families affected by the milk scandal was imprisoned for two and a half years.[49]

Internet Filtering

A spectrum of Internet filtering is found in Asia, ranging from some of the most pervasive censors of the Internet to relatively unfettered access. China and Burma rank among the most severe censors anywhere in the world. In these states, content related to opposition political movements, human rights, and pornography is widely blocked. While the scope and breadth of this blocking may not be found throughout the region, many other countries block similar content. For example, opposition political movements in Thailand and Vietnam are blocked, while Web sites deemed a threat to national security in South Korea and India are targeted. For some states, social content is the focus, with Indonesia and Pakistan concentrating their blocking on Web sites deemed offensive to religious values. Bangladesh, Malaysia, and the Philippines do not have systematic regimes of technical Internet filtering. However, Bangladesh in two separate incidents in 2010 blocked YouTube for hosting politically sensitive content[50] and Facebook for content deemed blasphemous.[51] In 2008, TMNet, a major ISP in Malaysia, performed a DNS block on the controversial Web site Malaysia Today following pressures from the government.[52]

There have been increasing challenges to the accessibility of online content from a variety of sources. Google had a highly public conflict with the government of China that culminated with the company refusing to continue censoring search results in the country.[53] Research in Motion (RIM) pushed back against India's efforts to gain access to the encrypted communications of BlackBerry users,[54] although it complied with requests from the Indonesian government to block pornography on the devices.[55]

Popular sites such as Facebook, YouTube, Flickr, and Wikipedia have all experienced some degree of control in South Korea, Pakistan, Bangladesh, and China. A December 2010 ruling by the Korean Communications Commission found that Facebook was in violation of the country's laws protecting personal information.[56] Responding to an online campaign to post drawings of the Prophet Mohammad in May 2010, the Pakistani government ordered ISPs to block access to Facebook for a month.[57] The campaign drew a similar response in Bangladesh, where the Telecommunications Regulatory Commission temporarily blocked Facebook until the site removed the offending images.[58] YouTube was targeted in Indonesia and Pakistan following the posting of a controversial film by Dutch lawmaker Geert Wilders.[59] The Web site was also blocked in Bangladesh "in the national interest" after video was posted of a contentious meeting between the prime minister and army officers.[60]

The blocking of such sites can be selective. OpenNet Initiative testing shows that South Korea has blocked the Twitter feed of the North Korean government, although North Korea's YouTube and Facebook pages were still accessible. In China, ONI testing in 2009 and 2010 found that the ISP CNLink had completely blocked Facebook and Twitter. Filtering practices have also extended to the mobile realm, with several

countries challenging the accessibility of content on BlackBerry devices. Research in Motion agreed to implement a content-filtering system in Indonesia to ensure compliance with the country's antipornography laws.[61] Similarly, BlackBerry users in Pakistan reportedly found content inaccessible as the Pakistan Telecommunication Authority ordered blasphemous material blocked.[62]

The practice of "just-in-time" blocking has also been prevalent in the region. During anniversaries of highly sensitive events, such as the 60th anniversary of the founding of the People's Republic of China, the 50th anniversary of the Tibet Uprising, and the 20th anniversary of the Tiananmen Massacre, China has seen increases in the level of blocking.[63] Thailand also experienced an increase in blocking during the 2010 red shirt demonstrations. Following the introduction of a state of emergency in April 2010, the government introduced strict measures to control the media, including Internet content, particularly content related to opposition parties or sympathetic to protesters. OpenNet Initiative testing confirmed that Thai ISPs targeted a selection of the 36 Web sites ordered blocked by the government during this period.[64]

Filtering is often not applied consistently within countries. Different ISPs sometimes filter different content, or do not filter content at all times. For example, ONI testing in Thailand found that filtering between the two tested ISPs, TRUE and TOTNET, was inconsistent, with neither provider blocking all the sites on the government block list. Internet service providers tested in Indonesia showed a similar lack of uniformity, with blocked content differing across providers. While there were some variations in the number of sites filtered by ISPs in countries such as Pakistan and India, the content was similar in nature. Providers tested in Burma showed a distinct difference in the precision of their filtering—testing results showed that Myanmar Post and Telecommunication (MPT) blocked specific pages while Yatanarpon Teleport (or Myanmar Teleport, formerly known as Bagan Cybertech) often blocked entire domains. Filtering has also been intermittent in countries such as Pakistan, Bangladesh, and Thailand where censorship occurs in response to a crisis or controversy.

The degree of transparency about blocking that users experience also varies between countries. China's system of IP blocking combined with keyword filtering, which is unique in the world, can resemble network problems. When accessing a blocked site, users receive a network-timeout error page, leaving them uncertain about whether content is in fact blocked. Other countries, including South Korea and some Indonesian ISPs, explicitly inform users that the content they are trying to access is blocked by government order.

Surveillance

Internet service providers in Asia are increasingly required to monitor their users' access and retain information about their usage. This practice can be seen most

prominently in Burma. Burmese Internet café owners are required to take screenshots of Web sites being visited.[65] Other countries, including China and Thailand, require Internet cafés to retain patron information and data usage records.

Surveillance has also extended into the mobile realm. The government of India confronted RIM over access to encrypted messages on BlackBerry devices, presenting the company with an ultimatum to grant access or face a ban on services.[66] Indonesia also expressed concern about its inability to monitor BlackBerry communications and requested that RIM set up local mirror servers to facilitate monitoring.

Some countries have expanded the requirements for Internet users to register with their real names before gaining access to services. In China, for example, users of some Web portals, Internet cafés, and mobile phones are required to present identification before gaining access.[67] Forum and chat-room users in South Korea have to register with their real names, a policy that led Google to disable features on the Korean-language version of YouTube to avoid the requirement.[68]

Cyber Attacks

Asian countries have also witnessed an increase in cyber attacks targeted at sensitive time periods, particularly during elections and anniversaries of key events. Burmese independent media Web sites regularly experience distributed denial of service (DDoS) attacks around anniversaries of political protests in the country such as the 2007 Saffron Revolution and the "8888" student uprising.[69] On October 25, 2010, two weeks before the first general elections in Burma since 1990, the primary ISP in the country, MPT, experienced large-scale DDoS attacks that significantly disrupted inbound and outbound traffic, rendering the Internet inaccessible.[70] The origin of and motivation behind the attacks remain unclear, but because of the timing there is speculation that they may be politically motivated. Controversial news site Malaysia Today reportedly faced a DDoS attack following published articles exposing government corruption.[71] In Vietnam, Web sites with content related to political reform hosted both within and outside of the country as well as dissidents in the country are frequently targets of DDoS attack.[72] For example, in April 2009, coinciding with the 24th anniversary of the fall of Saigon, the Web site of the Viet Tan, the Vietnam Reform Party, suffered a large-scale DDoS attack.[73]

Asian countries also continue to be primary sites for originating cyber attacks. In particular, a growing number of attacks have been attributed to sources originating from China, including targeted malware attacks on human rights groups[74] and media organizations,[75] and reports of attacks from numerous states such as Australia,[76] Japan,[77] Pakistan,[78] South Korea,[79] the United Kingdom,[80] and the United States.[81] Directly attributing any of these actions to the Chinese government is difficult, and the level of attacks sourced to the country should also be viewed within the context of China's growing Internet population, which is the biggest in the world.

Conclusion

While important variations exist across Asia, a trend of increasing controls in the context of growing connectivity is emerging in the region as a whole. This trend has not been limited to authoritarian countries. On the one hand, Burma, China, and Vietnam continue to expand and strengthen pervasive regimes of Internet controls, while on the other, South Korea imposes more restraints on the freedom of online speech than most other democracies, and Indonesia has begun to develop content controls for online pornographic material. This emerging trend reflects growing concerns over online content among governments in Asia as they struggle to balance the growth of information communication technologies with their interests of maintaining social stability and national security, as well as sustaining cultural values.

Both increasing connectivity and growing Internet controls have given rise to contestation over Asian cyberspace among different actors. Civil society actors, including netizens and activists, continue to use the Internet as a medium to broadcast their messages and to mobilize, organize, and resist state policies, while private actors struggle with obligations to governments in monitoring and filtering those very messages and forums of resistance. In India, such controls have tended to expand online civil society activism, while in Indonesia, a vibrant civil society including bloggers, media associations, women, and minority groups stands ready to challenge the imposition of regulations that could restrict online content freedoms.[82] In China, opposition from domestic and foreign PC makers as well as protests from angry netizens led the government to delay the "Green Dam" filtering program's installation in new computers.[83] At the same time, following a series of cyber attacks on its infrastructure and on e-mails of Chinese human rights activists, Google publicly challenged the country's filtering regime when it announced it would no longer comply with such regulations.[84]

Citizens also compete with one another over the shape of cyberspace. In Bangladesh, the promotion of an "Everyone Draw Mohammed Day" on Facebook gave rise to thousands of Bangladeshis protesting the social networking site and demanding an immediate ban, while other groups took to the streets after the country's telecommunication regulatory commission placed a temporary block on the Web site.[85] Other actors have sought to shape the Internet through cyber attacks that target opposition groups or forums for dissenting netizens. In Vietnam, cyber attacks on dissident groups and movements occur regularly, with the recent Vulcanbot and Vecebot botnets representing increasing sophistication of attacks.[86] There is some evidence that the perpetrators of the attacks are a pro–Vietnamese Communist Party hacking group concerned with reactionary online content.[87] In Burma, opposition media have seen a rise of cyber attacks on their Web sites, particularly on politically sensitive dates. Though some suspect such attacks to be state sanctioned, a lack of evidence makes state attribution difficult. Nonetheless, these attacks are consistent with the government's interest in strengthening Internet controls.

As states continue to promote information communication technologies and more citizens become connected to the Internet, netizens across the region may see a continuing rise of Internet controls. The contest over Asian cyberspace is expected to continue to intensify as actors with divergent interests compete with one another and vie for influence to shape the domain.

Notes

1. John D. Sutter, "Why Internet Connections Are Fastest in South Korea," CNN, March 31, 2010, http://articles.cnn.com/2010-03-31/tech/broadband.south.korea_1_broadband-plan-south-korea-broadband-internet?

2. International Telecommunication Union (ITU), "Internet Indicators: Subscribers, Users and Broadband Subscribers," 2009 figures, http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&ReportFormat=HTML4.0&RP_intYear=2009&RP_intLanguageID=1&RP_bitLiveData=False.

3. Darren Allan, "South Korea Tops Akamai Broadband Averages with 17 Mbps," Tech Watch, October 21, 2010, http://www.techwatch.co.uk/2010/10/21/south-korea-tops-akamai-broadband-averages-with-17mbps/.

4. ITU, "Internet Indicators: Subscribers, Users and Broadband Subscribers."

5. Note that mobile penetration rate is usually defined as the number of mobile subscriptions per person, so it can be higher than 100 percent. Paul Budde Communication Pty., Ltd., "Malaysia—Telecoms, Mobile and Broadband," May 2010, http://www.budde.com.au/Research/Malaysia-Telecoms-Mobile-and-Broadband.html.

6. Paul Budde Communication Pty., Ltd., "Vietnam—Telecoms, Mobile Broadband and Forecasts," June 2010, http://www.budde.com.au/Research/Vietnam-Telecoms-Mobile-Broadband-and-Forecasts.html.

7. Ibid.

8. ITU, "Internet Indicators: Subscribers, Users and Broadband Subscribers."

9. Ibid.

10. Ibid.

11. Ibid.

12. Ibid.

13. Ibid.

14. Ministry of Science and Information and Communication Technology, Government of the People's Republic of Bangladesh, "National Information and Communication Technology (ICT) Policy," October 2002, http://www.sdnbd.org/sdi/issues/IT-computer/itpolicy-bd-2002.htm.

15. ITU, "Internet Indicators: Subscribers, Users and Broadband Subscribers."

16. Paul Budde Communication Pty., Ltd., "Bangladesh—Telecoms, Mobile, Broadband and Forecasts," September 2010, http://www.budde.com.au/Research/Bangladesh-Telecoms-Mobile-Broadband-and-Forecasts.html.

17. ITU, "Internet Indicators: Subscribers, Users and Broadband Subscribers."

18. Paul Budde Communication Pty., Ltd., "India—Telecoms, Mobile, Broadband and Forecasts," July 2010, http://www.budde.com.au/Research/India-Telecoms-Mobile-Broadband-and-Forecasts.html.

19. ITU, "Internet Indicators: Subscribers, Users and Broadband Subscribers."

20. Paul Budde Communication Pty., Ltd., "PakistanTelecoms, Mobile Broadband and Forecasts," December 2010, http://www.budde.com.au/Research/Pakistan-Telecoms-Mobile-Broadband-and-Forecasts.html.

21. Wateen, "WiMAX," http://www.wateen.com/OurNetwork.aspx.

22. ITU, "Internet Indicators: Subscribers, Users and Broadband Subscribers."

23. Paul Budde Communication Pty., Ltd., "Indonesia—Telecoms, Mobile Broadband and Forecasts," March 2010, http://www.budde.com.au/Research/Indonesia-Telecoms-Mobile-Broadband-and-Forecasts.html.

24. ITU, "Mobile Cellular Subscriptions," http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/CellularSubscribersPublic&ReportFormat=HTML4.0&RP_intYear=2009&RP_intLanguageID=1&RP_bitLiveData=False.

25. "The Information Technology (Amendment) Act, 2008," February 5, 2009, http://www.mit.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf.

26. Vikas Asawat, "Information Technology (Amendment) Act, 2008: A New Vision through a New Change," March 2010, http://ssrn.com/abstract=1680152.

27. Aamir Attaa, "PTA to Devise Centralized Internet Censorship Practices," Pro Pakistani, June 23, 2010, http://propakistani.pk/2010/06/23/pta-to-devise-centralized-internet-censorship-practices/.

28. Ismira Lutfia, "Indonesia Web Monitoring Plan Panned," *Jakarta Globe*, February 16, 2010, http://www.thejakartaglobe.com/home/indonesia-web-monitoring-plan-panned/358890; Aubrey Belford, "Sex Tape Scandal Fixates Indonesia," *New York Times*, June 13, 2010, http://www.nytimes.com/2010/06/14/world/asia/14iht-sextape.html; and ICT Watch, "Indonesia Censorship," brief report presented at OpenNet Initiative Global Summit, Ottawa, Canada (June 2010), http://www.slideshare.net/donnybu/indonesian-internetcensorshipreport2010.

29. Siriphon Kusonsinwut, Sawatree Suksri, and Oraphin Yingyongpathana, "Situational Report on Control and Censorship of Online Media, through the Use of Laws and the Imposition of Thai State Policies," iLaw, http://ilaw.or.th/node/632.

30. Gillian Wong, "China Set to Tighten State-Secrets Law Forcing Internet Firms to Inform on Users," *Washington Post*, April 28, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/04/27/AR2010042704503.html.

31. "Law of the People's Republic of China on Guarding State Secrets," adopted at the Third Meeting of the Standing Committee of the Seventh National People's Congress on September 5, 1988, and revised at the 14th Session of the Standing Committee of the 11th National People's Congress on April 29, 2010, http://www.npc.gov.cn/npc/xinwen/2010-04/29/content_1571588.htm. Unofficial English translation is available at: http://www.hrichina.org/public/PDFs/PressReleases/20101001-StateSecretsLaw-EN.pdf.

32. Human Rights Watch, "World Report 2008—Bangladesh," January 31, 2008, http://www.unhcr.org/refworld/docid/47a87bf8c.html.

33. Tarek Mahmud, "Cyber Crime Detour: Facebook?" *Daily Star*, June 5, 2010, http://www.thedailystar.net/law/2010/06/01/life.htm.

34. "Draft Bill to Control Pornography to Be Placed at Next Cabinet Meeting for Approval," New Age, November 12, 2010, http://www.newagebd.com/2010/nov/12/nat.html; and Dhaka Mirror, "Law to Curb Cyber Crimes in Cards," October 13, 2010, http://www.dhakamirror.com/?p=18559.

35. Heru Andriyanto, "Teenager May Be Charged for Facebook Defamation," *Jakarta Globe*, July 9, 2009, http://www.thejakartaglobe.com/national/teenager-may-be-charged-for-facebook-defamation/317034.

36. Ardhi Surayadhi, "Pemerintah Akhirnya Keluarkan Perintah Blokir [Government Finally Removes the Command Block]" [Indonesian], DekiINET, http://us.detikinet.com/read/2010/05/20/135758/1360788/398/pemerintah-akhirnya-keluarkan-perintah-blokir.

37. Aubrey Belford, "Indonesia Finds Banning Pornography Is Difficult," *New York Times*, August 2, 2010, http://www.nytimes.com/2010/08/02/technology/02iht-indoporn02.html.

38. Alecks Pabico, "Blogspot Blanket Ban in Pakistan Appears to Be Lifted," Free Expression in Asian Cyberspace, May 4, 2006, http://freeexpressionasia.wordpress.com/2006/05/04/blogspot-blanket-ban-appears-to-be-lifted.

39. Telecommunications Business Act (wholly amended by presidential decree no. 13558 on August 10, 1991); and Decisions of the Korean Constitutional Court, Opinion14–1 KCCR 616, 99Hun-Ma480, June 27, 2002.

40. Malaysian Communications and Multimedia Act, 1998.

41. "Web Censoring Needs a Debate," *Bangkok Post*, January 6, 2009, http://www.bangkokpost.com/opinion/opinion/9202.

42. Kusonsinwut et al., "Situational Report on Control and Censorship of Online Media."

43. Charles Lourdes, "Six to Be Charged for Insulting Perak Sultan via Blogs, Postings (Update 2)," *The Star*, March 12, 2009, http://thestar.com.my/news/story.asp?sec=nation&file=/2009/3/12/nation/20090312194041.

44. Nurul Huda Jamaluddin, "Blogger 'Hassan Skodeng' to Face Charge Tomorrow," *Malay Mail*, September 1, 2010, http://www.mmail.com.my/content/48211-blogger-hassan-skodeng-face-charge-tomorrow.

45. International Freedom of Expression Exchange, "Hundreds of Police Shut Down Pro-opposition Newspaper," June 9, 2010, http://www.ifex.org/bangladesh/2010/06/09/opposition_hunt/.

46. Bae Ji-sook, "Prosecution Investigates Groundless Rumormongers," *Korea Times*, November 24, 2010, http://www.koreatimes.co.kr/www/news/nation/2010/11/117_76912.html.

47. Song Jung-a, "South Korean Court Rules on Internet Law," *Financial Times*, December 28, 2010, http://www.ft.com/cms/s/0/38b354a4-126d-11e0-b4c8-00144feabdc0.html.

48. Damian Grammaticas, "Chinese Woman Jailed over Twitter Post," BBC News, November 18, 2010, http://www.bbc.co.uk/news/world-asia-pacific-11784603.

49. Andrew Jacobs, "China Sentences Activist in Milk Scandal to Prison," *New York Times*, November 10, 2010, http://www.nytimes.com/2010/11/11/world/asia/11beijing.html.

50. "Bangladesh Imposes YouTube Block," BBC News, March 29, 2010, http://news.bbc.co.uk/2/hi/7932659.stm.

51. "Bangladesh Blocks Facebook over Mohammed Cartoons," Agence France-Presse, May 29, 2010, http://www.google.com/hostednews/afp/article/ALeqM5ju8Kku2aAuieZmu1g3uUvBOFpHNA.

52. Nurbaiti Hamdan and Cheok Li Peng, "ISPs Ordered to Cut Access to *Malaysia Today* Website," August 28, 2008, *The Star*, http://thestar.com.my/news/story.asp?file=/2008/8/28/nation/22187596&sec=nation.

53. Andrew Jacobs and Miguel Helft, "Google, Citing Attack, Threatens to Exit China," *New York Times*, January 12, 2010, http://www.nytimes.com/2010/01/13/world/asia/13beijing.html?scp=3&sq=google%20china&st=cse.

54. "RIM Says No Access to Corporate Email in India," Reuters, January 27, 2011, http://in.reuters.com/article/2011/01/27/idINIndia-54445120110127.

55. "Blackberry Maker Says Will Filter Porn to Meet Indonesia Rules," Reuters, January 10, 2011, http://ca.reuters.com/article/businessNews/idCATRE7092DK20110110.

56. Martyn Williams, "Facebook in Breach of Korean Privacy Laws, Says Regulator," Computer World, December 8, 2010, http://www.computerworld.com/s/article/9200458/Facebook_in_breach_of_Korean_privacy_laws_says_regulator.

57. Waqar Gillani, "Pakistan: Court Blocks Facebook," *New York Times,* May 19, 2010, http://www.nytimes.com/2010/05/20/world/asia/20briefs-Pakistan.html.

58. "Bangladesh Blocks Facebook over Mohammed Cartoons," Agence France-Presse, May 29, 2010, http://www.google.com/hostednews/afp/article/ALeqM5ju8Kku2aAuieZmu1g3uUvBOFpHNA.

59. "Indonesia Seeks to Block YouTube over Anti-Koran Film," Reuters, April 2, 2008, http://uk.reuters.com/article/idUKJAK29880220080402; "Indonesia Blocks YouTube to Protest Islam

Film," CNN, April 8, 2008, http://www.cnn.com/2008/WORLD/asiapcf/04/08/indonesia.youtube/index.html.

60. "Bangladesh Imposes YouTube Block," BBC News, March 29, 2010, http://news.bbc.co.uk/2/hi/7932659.stm.

61. "Blackberry Maker Says Will Filter Porn to Meet Indonesia Rules," Reuters.

62. Muhammad Yasir, "BlackBerry Internet Services Yet to Be Restored," *Daily Times*, July 18, 2010, http://www.dailytimes.com.pk/default.asp?page=2010\07\18\story_18-7-2010_pg5_4.

63. Committee to Protect Journalists, "National Day Triggers Censorship, Cyber Attacks in China," September 22, 2009, http://cpj.org/2009/09/national-day-triggers-censorship-cyber-attacks-in.php; Tania Branigan, "China Blocks Twitter, Flickr and Hotmail Ahead of Tiananmen Anniversary," *The Guardian,* June 2, 2009, http://www.guardian.co.uk/technology/2009/jun/02/twitter-china; and "China Should Allow Access to Tibetan Areas," Foreign Correspondents' Club of China Statement, March 9, 2009, http://www.fccchina.org/2009/03/09/china-should-allow-access-to-tibetan-areas.

64. Anuchit Nyguen, "Thai Government Blocks Protest Web Site after Emergency Decree," *Bloomberg Business Week*, 7 April 2010, http://www.businessweek.com/news/2010-04-07/thai-government-blocks-protest-web-site-after-emergency-decree.html.

65. Kanbawza Win, "Fighting the Very Concept of Truth," *Asian Tribune*, October 1, 2010, http://www.asiantribune.com/news/2010/10/01/fighting-very-concept-truth.

66. Devidutta Tripathy and Krittivas Mukherjee, "RIM Gives India Access but Not to Secure E-mails," Reuters, January 13, 2011, http://www.reuters.com/article/2011/01/13/us-blackberry-india-idUSTRE70C1G920110113.

67. "Top 10: Please Show Your ID," *China Daily*, December 10, 2010, http://www2.chinadaily.com.cn/china/2010-12/10/content_11684998.htm.

68. Antone Gonsalves, "Google Scales Back YouTube Korea," *Information Week*, April 13, 2009, http://www.informationweek.com/news/internet/google/showArticle.jhtml?articleID=216500489.

69. See Nart Villeneuve and Masashi Crete-Nishihata, "Control and Resistance: Attacks on Burmese Opposition Media," chapter 8 in this volume.

70. Craig Labovitz, "Attack Severs Burma Internet," Arbor Networks, November 3, 2010, http://asert.arbornetworks.com/2010/11/attac-severs-myanmar-internet.

71. "M'sia Today Blocked 'To Stop Release of Documents,'" Malaysiakini, September 10, 2010, http://malaysiakini.com/news/142385.

72. Human Rights Watch, "Vietnam: Stop Cyber Attacks against Online Critics," May 26, 2010, http://www.hrw.org/en/news/2010/05/26/vietnam-stop-cyber-attacks-against-online-critics.

73. Viet Tan, "Denial of Service Cyber Attacks by the Vietnamese Government," April 27, 2010, http://www.viettan.org/spip.php?article9749.

74. Nart Villeneuve, "Human Rights and Malware Attacks," Nart Villeneuve: Malware Explorer, July 29, 2010, http://www.nartv.org/2010/07/29/human-rights-and-malware-attacks; Danny O'Brien, "That Nobel Invite? Mr. Malware Sent It," Committee to Protect Journalists, November 10, 2010, http://www.cpj.org/internet/2010/11/that-nobel-invite-mr-malware-sent-it.php.

75. "Warning on Fake Emails Targeting News Assistants," Foreign Correspondents' Club of China, September 21, 2009, http://www.fccchina.org/2009/09/21/warning-on-fake-emails-targeting-news-assistants; Nart Villeneuve and Greg Walton, "Targeted Malware Attack on Foreign Correspondents Based in China," Nart Villeneuve: Malware Explorer, September 29, 2009, http://www.nartv.org/2009/09/28/targeted-malware-attack-on-foreign-correspondent%E2%80%99s-based-in-china.

76. Brett Winterford, "Optus Customers Hit by China DDOS Attack," *SC Magazine*, April 15, 2010, http://www.securecomputing.net.au/News/172229,optus-customers-hit-by-china-ddos-attack.aspx; and Asher Moses, "Chinese Cyber Attackers Hit Optus," *Sydney Morning Herald*, April 15, 2010, http://www.smh.com.au/technology/security/chinese-cyber-attackers-hit-optus-20100415-sgm8.html.

77. "Chinese Hackers Suspected of DDoS Attacks against Japan," The New New Internet, September 27, 2010, http://www.thenewnewinternet.com/2010/09/27/chinese-hackers-suspected-of-ddos-attacks-against-japan; and "Japan Suspects Cyber Attacks Amid China Row: Media," Agence France-Press, September 17, 2010, http://www.google.com/hostednews/afp/article/ALeqM5jrJX2uRX7gxO3zPa_dO-rE0FPbnA.

78. Rajeev Deshpande and Vishwa Mohan, "Pakistan, China Hackers Tried to Deface CWG Sites," *Times of India*, October 16, 2010, http://timesofindia.indiatimes.com/india/Pakistan-China-hackers-tried-to-deface-CWG-sites/articleshow/6755521.cms; and Indrani Bagchi, "China Mounts Cyber Attacks on Indian Sites," *Times of India*, May 5, 2008, http://timesofindia.indiatimes.com/India/China-mounts-cyber-attacks-on-Indian-sites/articleshow/3010288.cms.

79. "S. Korean Government Website Hit by Cyber Attacks," Agence France-Presse, June 9, 2010, http://www.google.com/hostednews/afp/article/ALeqM5j-cLHwEp033Jo3lRnOJSFM9L3z6Q.

80. David Hencke, "Whitehall Plans New Cyber Security Centre to Deter Foreign Hackers," *The Guardian*, June 14, 2009, http://www.guardian.co.uk/technology/2009/jun/14/government-security-cyber-crime-hacking.

81. Sam Diaz, "Law Firm That Sued Chinese Government Reports Cyber Attack," ZDNet, January 13, 2010, http://www.zdnet.com/blog/btl/law-firm-that-sued-chinese-government-reports-cyber-attack/29533; and Lolita Baldor, "Pentagon Takes Aim at China Cyber Threat," ABC News, August 19, 2010, http://abcnews.go.com/Politics/wireStory?id=11439149.

82. "Indonesia Passes Anti-porn Bill," BBC News, October 30, 2008, http://news.bbc.co.uk/2/hi/7700150.stm; Peter Gelling, "Indonesia Passes Broad Anti-pornography Bill," *New York Times*, October 30, 2008, http://www.nytimes.com/2008/10/30/world/asia/30iht-indo.1.17378031.html; "Press Freedom Victim of Defamation Law's 'Inverted Logic,' Journalists Say," *Jakarta Globe,*

May 6, 2009, http://www.thejakartaglobe.com/justAdded/press-freedom-victim-of-defamation-laws-inverted-logic-journalists-say-/275348.

83. Joe McDonald, "China Eases Internet Restrictions," Huffington Post, June 30, 2009, http://www.huffingtonpost.com/2009/07/01/china-eases-internet-rest_n_223895.html.

84. "Google 'May Pull Out of China after Gmail Cyber Attack,'" BBC News, January 13, 2010, http://news.bbc.co.uk/2/hi/8455712.stm.

85. "Facebook Blocked," *Daily Star*, May 30, 2010, http://www.thedailystar.net/newDesign/news-details.php?nid=140613; and "Lift Ban on Facebook," *Daily Star*, May 31, 2010, http://www.thedailystar.net/newDesign/news-details.php?nid=140815.

86. Viet Tan, "Denial of Service Cyber Attacks by the Vietnamese Government"; Neel Mehta, "The Chilling Effects of Malware," Google Online Security Blog, March 30, 2010, http://googleonlinesecurity.blogspot.com/2010/03/chilling-effects-of-malware.html; George Kurtz, "Vietnamese Speakers Targeted in Cyberattack," McAfee, March 30, 2010, http://siblog.mcafee.com/cto/vietnamese-speakers-targeted-in-cyberattack; SecureWorks' Counter Threat Unit, "Vecebot Trojan Analysis," SecureWorks, October 28, 2010, http://www.secureworks.com/research/threats/vecebot.

87. SecureWorks' Counter Threat Unit, "Vecebot Trojan Analysis"; Viet Tan, "Denial of Service Cyber Attacks by the Vietnamese Government."

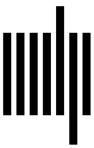
Access Contested

Security, Identity, and Resistance in Asian Cyberspace

Edited by: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan L. Zittrain

Citation:

Access Contested: Security, Identity, and Resistance in Asian Cyberspace
Edited by: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan L. Zittrain
DOI: 10.7551/mitpress/9780262016780.001.0001
ISBN (electronic): 9780262298919
Publisher: The MIT Press
Published: 2011



The MIT Press

The online edition of this work is available from IDRC and at http://www.access-contested.net.

International Development Research Centre
PO Box 8500, Ottawa, ON K1G 3H9, Canada
info@idrc.ca / www.idrc.ca <http://www.idrc.ca>
ISBN 978-1-55250-507-6 (IDRC e-book)

This book was set in Stone Sans and Stone Serif by Toppan Best-set Premedia Limited. Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data

Access contested : security, identity, and resistance in Asian cyberspace / edited by Ronald Deibert . . . [et al.].
p. cm. — (Information revolution and global politics)
Includes bibliographical references and index.
ISBN 978-0-262-01678-0 (hardcover : alk. paper) — ISBN 978-0-262-51680-8 (pbk. : alk. paper)
1. Cyberspace—Government policy—Asia. 2. Computer security—Asia. 3. Computers—Access control—Asia. 4. Internet—Government policy—Asia. 5. Internet—Censorship—Asia. I. Deibert, Ronald.
HM851.A253 2011
303.48′33095—dc23

2011031273

10 9 8 7 6 5 4 3 2 1