Asia Pacific Foundation of Canada
Fondation Asie Pacifique du Canada

September 13, 2011

CANADA-ASIA AGENDA

www.asiapacific.ca Series Editor Brian Job Associate Editor Trang Nguyen Issue 20

Asian Cyberspace on the Rise: Challenges and Opportunities for Canada

By Ronald Deibert

As the ingenuity and creativity of information and communication technology flourishes in Asia, it faces broadening cyberspace controls from some of the world's most restrictive regimes. The future of cyberspace lies with Asia, and Ron Deibert argues Canadians should pay attention. This piece highlights how countries are responding to the challenges and opportunities of growing innovation in the region. It also outlines the limited role Canada can play in shaping developments of cyberspace governance and security in Asia which will have far reaching implications in the future.

Introduction

Asia now comprises nearly 45% of the world's Internet population.[1] China alone – home to the world's largest number of Internet users - makes up more than half of the region's entire Internet population.[2] The China Internet Network Information Centre estimates that China's online population rose 6% to 485 million in 2011.[3] What is remarkable is that nearly two thirds of Chinese, and close to 70% of the Asian population as a whole, are not yet even online.[4] As this growth continues, the culture of global cyberspace will change. The concept of "Asian values" may have limited merit in academic circles, but there is no doubt that a sociological and political shift will occur that will affect cyberspace writ large. With these new users will come new ways of using and governing cyberspace, both at home and abroad, which will have far reaching implications for the world.

The region's extraordinary diversity of ethnic groups, cultures, ecologies, and political systems belie simplistic observations. Yet it is also this very diversity and dynamism that makes the region so potent a force in global affairs, particularly in regard to Asian cyberspace. The Asian region not only contains some of the most diverse cyberspace policies, ranging from free-wheeling zones of entrepreneurialism to islands of state control, it is the fastest growing region on the planet for connectivity to cyberspace.

This article examines some of the characteristics of cyberspace governance and security in Asia, as countries respond in different ways to the challenges and opportunities of exploding growth and innovation. It then considers how Canada might exercise its limited influence to shape developments in Asian cyberspace. The future of cyberspace lies with Asia, which is why Canadians should pay attention.


Photo Credit: Donna Santos

About The Author

Ronald Deibert is Professor of Political Science and Director of the Canada Centre for Global Security Studies and the Citizen Lab at the Munk School of Global Affairs, University of Toronto and the co-editor of "Access Contested: Security, Identity and Resistance in Asian Cyberspace", (MIT Press: 2011). He is a co-founder and principal investigator of the OpenNet Initiative and InfoWar Monitor projects.

Cyberspace Governance in Asia

Governance of cyberspace in Asia is as extraordinarily diverse as the countries that make up the region. But the countries of Asia are coming online in a different geopolitical context than the early adopters of the West. "Cyber security" was largely unheard of in the early days of the Internet; today it is the bottom line for governments of all stripes. Moreover, the rapidly developing countries of Asia arguably have been characterized by a greater tradition of and tolerance towards state involvement in the economy and society than the liberal democracies of the West, who have approached cyberspace, until recently, in a "hands off" manner. For both of these reasons, we can expect Asian governments to be more comfortable exercising a broad range of controls over cyberspace as Information and Communication Technology (ICT) growth continues in an accelerated fashion.

Photo Credit: istockphoto.com

Presently, Asia includes some of the world's most tightly restrictive countries for freedom of speech and access to information, including China, Burma, Vietnam, and North Korea. While many have speculated that there would be a gradual easing of authoritarianism with the growth of the Internet, the opposite tendency appears to be the case. China's well known system of filtering access to information online, known colloquially as the "Great Firewall of China," has been supplemented by a complex system of ever-deepening information controls ranging from informal pressures to formal laws and a myriad of private sector regulations designed to capitalize on information flows while minimizing their adverse social and political impacts.[5] Private sector actors offering services in China are obliged to follow rules on acceptable content hosting, and comply with extensive surveillance of their customers on behalf of China's security services. Google found this out through the course of its roughly five year engagement in the country, leading to its well known and very public 2010 spat and the withdrawal of its operations out of the mainland to Hong Kong. The spat did little to de-rail China's intentions to control the Internet, and may have even accelerated processes of ICT nationalization.

Vietnam follows a similar tack as China, building out multi-tiered information regulations, pressuring private sector actors to comply with censorship and surveillance requests, and jailing dissidents and writers. Burma/Myanmar and North Korea are of course among the world's most repressive regimes and show every sign of maintaining those policies as the tiny fraction of their population moves online incrementally and in a rigidly controlled manner. Both countries have plans to develop "national intranets" through which only pre-approved "white listed content" can be accessed by citizens. China, Vietnam, and Burma all also appear to be tolerant towards, if not openly supportive of, targeted electronic attacks, including cyber espionage and denial of service, against the websites of adversaries, and opposition and human rights groups based abroad[6] - a trend mirrored in the Middle East and North Africa, and especially Iran and Syria.

It may seem unsurprising that these authoritarian regimes are bolstering cyberspace controls. But non-authoritarian Asian countries also appear to be heading in the same direction. While South Korea leads the world in Internet connectivity, the government maintains a strict Internet censorship and surveillance regime justified on the basis of national security.[7] Although Singapore has long been assumed to be censoring Internet content, the government actually requires ISPs to block only a handful of symbolic pornographic sites.[8] However, it does maintain a very strict libel regime that creates a chilling effect on public discourse. Both Pakistan and India now censor a growing list of political and national security web sites, often in ways that are highly controversial and lacking in transparency and accountability.[9] One Pakistani ISP recently required users of its service to log into a special proxy account that prevented them from searching for anything containing the keywords of the President of Pakistan, Asif Ali Zardari.[10] In another episode, 13 Pakistani ISPs blocked access to the website of Rolling Stone Magazine (rollingstone.com) because of an article containing reference to Pakistan's military spending.[11]

The justification of protecting "public morality" or controlling "blasphemy" to censor the Internet is, in fact, growing throughout the region. Thailand has stepped up its Internet censorship regime, including exercising lese majeste laws, to imprison an increasing number of those who publish content online that is critical of the ruling monarchy.[12] In

Cambodia, the government used a morality pretext to require ISPs and mobile phone operators to block access to political opposition websites.[13] Even among countries that traditionally have had little to no Internet censorship, such as the Philippines, Malaysia, Japan, and Taiwan, pressures are mounting to control the Internet because of concerns about cyber crime, copyright infringement, public morality and decency, or the enforcement of slander and libel laws.

Asian cyberspace is shaped not only by national-level policies; governments of the region are developing foreign policies for cyberspace governance, including coordination at regional and global levels that will have an influence on the character of cyberspace internationally. Some of this foreign policy engagement is coordinated, such as through the Shanghai Cooperation Organization (SCO), which includes Asian states, Russia and some other countries of the Commonwealth of Independent States (CIS), and several important "observer" countries, such as Iran. Although the meetings of the SCO tend to be highly secretive, there are clear indications that the organization is used as a forum to coordinate counter-terrorism strategies, which are broadly defined by the members to include anti-regime popular mobilizations of the type that characterized the "Arab Spring". Insofar as this coordination succeeds, it will extend and normalize the paradigm of "information security" favored by Russia and China throughout Asia and neighboring areas, creating further tension with the "Internet Freedom" agenda of the United States and its allies, which support materially and otherwise the very groups the SCO aims to neutralize.

These differences are increasingly playing themselves out in international Internet governance forums where China, India, and other Asian countries are steering policies towards the legitimization of their national-style cyberspace controls. Part of that agenda includes limiting the involvement of civil society stakeholders in governance and standard-setting bodies, like ICANN, the Internet Governance Forum, and others, and implementing a more traditional state-led regime of cyberspace governance. Although resisted by netizens, the private sector, and powerful governments, especially the United States, the agenda does find reception in the United Nations and in particular with the head of the International Telecommunications Union, Hamid Toure, and resonates among many like-minded countries in South America, Central Asia, and Africa.[14]

Normalizing and extending Internet controls is not merely a function of foreign policy. Norms and values can be carried internationally by the private sector as well. Asian economies are almost synonymous with ICT innovation, but a portion of that market segment is also growing around products and services that assist governments in implementing cyberspace controls as part of a growing cyber security military industrial complex. Probably the most notorious of these is the Chinese IT giant Huawei, which has won contracts for surveillance and other control technologies in Belarus, Nigeria, and the Middle East. The company has also been reportedly working with Iranian companies to jointly develop a "national search engine" for the Iranian market similar to that being developed in China. Concerns about Huawei's links to the Chinese military and the national security issues that arise thereof have prompted reviews of the sale of its technology in the United States, the United Kingdom, and India.[15] But as Asian national markets for cybersecurity technologies mature and saturate, we can expect home-grown companies like Huawei to join their North American and European counterparts in offering products and services abroad to a growing number of governments implementing their own cyberspace control regimes.

Cybersecurity in Asia

One area that is likely to be an important centre of gravity for developments in Asian cyberspace concerns cyber security. For most, cyber security in the context of Asia conjures up images of Chinese-based cyber espionage networks, and repeated high-level breaches of corporate and government assets in the United States, Canada, and Europe. It is hard to deny this dominant motif when the evidence on the origins of the attacks points consistently back to mainland Chinese Internet space. In what is a highly typical episode, **recent disclosures from the Canadian government indicated that breaches of the Canadian Treasury Department and at least one other Canadian government agency, which knocked Internet access offline for employees for months, traced back to Chinese IP addresses.[16]** China's official response in that affair was identical to others of its ilk: to deny any official involvement, and claim that they are as much victimized by cyber crime as other countries.

While some may look upon these official statements cynically, there is a kernel of truth in them. Statistics on cyber crime suggest that China and most other rapidly ICT-developing Asian countries are massive breeding grounds of the types of vulnerabilities and insecurities in which cyber crime thrives. It should come as no surprise that much of the mali-

cious activity discovered on networks anywhere in the world traces back to Asian cyberspace. Asian government agencies themselves are indeed victimized as much, if not more, than anywhere else. In a remarkable study by the American security researcher Drew Beresford, a scan of Chinese public networks showed gaping vulnerabilities across the spectrum, attributed by Beresford in part to the widespread use of pirated Windows operating systems.[17] The combination of pirated software, insecure infrastructure, poor policing, and rapidly growing usage combines like a kind of petri dish for underground experimentation and exploitation. To give just one example, it is estimated as much as 70% of the computers in Taiwan may be infected with malicious software.[18]

It is highly unlikely that Chinese security services do not exploit and even cultivate the illicit gains of cyber crime for strategic and economic advantage - just as, no doubt, do the security services of many other countries worldwide. But as the Chinese economy becomes more and more dependent on global flows of information, it will have a growing stake in securing both its own infrastructure, and that based abroad, creating an invariable tension in strategic policy.

Implications for Canada

Influencing the shape and direction of these tendencies for a country like Canada is not going to be easy as our influence is limited and must be targeted carefully to be effective. While many might be tempted to tackle the rights issues head on, smaller, more practical steps maybe more effective and realistic. For example, the Canadian Embassy in Beijing recently launched a micro-blogging platform, which was subject to censorship when Canadian officials placed a link to the full text of the controversial Chinese-Canadian deportation case.[19] While the media focused on the censorship of the one posting, largely overlooked was the fact that the platform itself has been permitted in the first place, offering a channel of direction communications between the Canadian government and Chinese citizens.

Likewise, the cyber security, rather than the "Internet freedom," agenda, may provide the most important engagement opportunity for Canada and other liberal democracies in Asia. Asian governments, and their law enforcement and computer security response teams, will invariably have an interest in greater coordination to control the exploding world of cyber crime that affects their own core interests, as much as the rest of the world. Dealing with these problems can be done in a heavy-handed way that diminishes rights online, or it can be done in a way that respects the rule of law, public accountability, and transparency. Canada can lead the way on the latter, but only if it sets its own house in order accordingly. Chinese and other computer security response teams should be brought into a common conversation on how to cooperate on cyber crime, both domestically and abroad. Lessons from the Cold War, where Russian and American nuclear scientists engaged in a dialogue that led to gradual mutual trust and understanding at higher levels, can be replicated in the Asian cyber security arena, where tensions and suspicions run high.

Internet Governance Forum, held in Rio de Janeiro in 2007.

The rights agenda is more effectively dealt with in a multilateral manner. Canada needs to be a strong voice at the many international Internet governance forums and standard setting bodies to counter-act the growing weight of nationalized controls seeping in across the board. Presently, we are not. In light of the fact that there is no one "centre" of cyberspace governance, policy will have to be coordinated across many different forums, from APEC and ASEAN to the G8 and G20, the Internet Governance Forum and others, in a strong and credible fashion. Our message, and policy engagement, which will need to be coordinated across several Departments, should be consistent with a vision of cyberspace that is both open and secure, but placing emphasis on economic self-interest and the future interdependence all nations have on open networks. To that end, we should insist that all companies, including Canadian companies, operate in accordance with basic human rights standards abroad and avoid facilitating enclosure on the Internet. We should push Internet censorship issues to legal forums, like the World Trade Organization for example, where they can be effectively dealt with in a legal, rather than rhetorical level, and can be progressively subject to greater accountability.

Where the long-term balance tips in Asia around cyberspace governance is an open question, and difficult to predict with certainty. Present trends are tilted in the direction of greater cyberspace controls, and a variety of indicators suggest these norms will be conveyed internationally as Asian influence expands. But Asian cyberspace is a dynamic ecosystem exploding in numbers and a challenge for even the most ambitious governments to tame. It is difficult to anticipate how those controls will be met with the burgeoning number of young Asia Internet users who have shown remarkable ingenuity, creativity, and even in China a remarkable capacity to evade the heavy hand of the censors. Asian cyberspace is thus likely to be a contested ecosystem among governments, the private sector, and civil society.

OpenNet Asia

The OpenNet Initiative (http://opennet.net/) is a collaborative partnership of three institutions: the Citizen Lab at the Munk School of Global Affairs, University of Toronto; the Berkman Center for Internet & Society at Harvard University; and the SecDev Group (Ottawa).The aim of the ONI is to investigate, expose and analyze Internet filtering and surveillance practices in a credible and non-partisan fashion. To achieve these aims, the ONI employs a unique multi-disciplinary approach that includes:

* Development and deployment of a suite of technical enumeration tools and core methodologies for the study of Internet filtering and surveillance;

* Capacity-building among networks of local advocates and researchers;

* Advanced studies exploring the consequences of current and future trends and trajectories in filtering and surveillance practices, and their implications for domestic and international law and governance regimes.

Since 2002, the ONI has performed comprehensive studies on Internet filtering in forty countries, including eleven in Asia. With the support of the International Development Research Centre (IDRC) Canada, the ONI was tasked in 2009 to engage academic, policy, and civil society stakeholders in Asia to build institutional capacity and networked resources to conduct research and public policy advocacy around cyberspace controls. The results of that engagement are featured in the forthcoming volume with MIT Press, "Access Contested: Security, Resistance and Identity in Asian Cyberspace" (edited by Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain). Access Contested features ten thematic chapters, an overview of the Asian region, and ten extensive country reports based on the research of the ONI in Asia.

1. Internet World Stats, "Internet Usage in Asia", available at: http://www.internetworldstats.com/stats3.htm.

2. Ibid

3. Total Telecom, "China's Internet population hits 485 million", posted on July 19, 2011. Available at: http://www.totaltele.com/view.aspx?ID=466349.

4. Internet World Stats, "Internet Usage in Asia", available at: http://www.internetworldstats.com/stats3.htm.

5 . Open Net Initiative, "Country Profile: China (2009)", available at: http://opennet.net/research/profiles/china.

6. See "Hal Roberts, Ethan Zuckerman, and John Palfrey, "Interconnected Contests: Distributed Denial of Service Attacks and Other Digital Control Measures in Asia," and Nart Villeneuve and Masashi Crete-Nishihata, "Control and Resistance: Attacks on Burmese Opposition Media," in Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, eds. Access Contested: Security, Resistance, and Identity in Asian Cyberspace, (Cambridge: MIT Press, 2011).

7. Open Net Initiative, "Country Profile: South Korea (2010)", available at: http://opennet.net/research/profiles/south-korea.

8. Open Net Initiative, "Country Profile: Singapore (2007)", available at: http://opennet.net/research/profiles/singapore.

9. For more details please see: Open Net Initiative, "Country Profile: India", http://opennet.net/research/profiles/india, and "Country Profile: Pakistan", http://opennet.net/research/profiles/pakistan.

10. Jillian C. York, "Pakistan escalates its Internet censorship", Al Jazeeara, July 26, 2011. Available at: http://english.aljazeera.net/indepth/opinion/2011/07/20117251113105899 12.html.

11. ibid

12. Open Net Initiative, "Country Profile: Thailand". Available at: http://opennet.net/research/profiles/thailand.

13. Global Voices, "Cambodia: Who ordered the Blocking of Opposition Websites?", posted on February 27, 2011. http://globalvoicesonline.org/2011/02/27/cambodia-who-ordered-the-blocking-of-opposition-websites/

14. For discussion, see Milton Mueller, "China and Global Internet Governance: A Tiger by the Tail," in Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, eds. Access Contested: Security, Resistance, and Identity in Asian Cyberspace, (Cambridge: MIT Press, 2011).

15. Michael R. Wessel and Lary M. Wortzel, "The Huawei Security Threat", The Wall Street Journal. http://online.wsj.com/article/SB10001424052748704300604575555121880239064.html.

16. Greg Weston, "Foreign Hackers attack Canadian Government", CBC News, February 16, 2011. http://www.cbc.ca/news/politics/story/2011/02/16/pol-weston-hacking.html.

17. Paul Roberts, "Glass Dragon: China's Cyber Offense Obscures Woeful Defense," Threatpost (April 27, 2011), http://bit.ly/dPQr0A

18. Panda Security, "PandaLabs Q1 Report: China, Thailand and Taiwan World's most infected Countries, with nearly 70 percent of all computers riddled by Malware", April 5, 2011, http://bit.ly/ohRwej

19. Mark Mackinnon, "Canada's embassy posting on Lai Changxing taken off Chinese site", Globe and Mail, August 6, 2011. http://bit.ly/qJ1lyH